gemeente Heemskerk

Overkoepelend beleid Privacy & gegevensbescherming Gemeente Heemskerk 2016

september 2016

OD/2016/158442
Z01FBB92470

Inhoudsopgave

Geregistreerd onder nummer OD/2016/165423

Wettelijke grondslag:
Wet bescherming persoonsgegevens, Algemene Verordening Gegevensbescherming

Inleiding

De gemeente Heemskerk verzamelt en bewerkt persoonsgegevens in verband met de dienstverlening aan burgers en bedrijven. Het gaat bijvoorbeeld om de gegevens in de gemeentelijke basisregistratie personen, de registratie van uitkeringsgerechtigden, het bijhouden van gegevens uit bouwaanvragen en het verwerken van gegevens van mensen die een voorziening hebben aangevraagd.
Deze verwerking van persoonsgegevens leidt er toe dat de gemeente van alles over de burger te weten komt, wat inbreuk maakt op de persoonlijke levenssfeer van de burger. Dat gevaar speelt een grotere rol, naarmate de gemeente meer soorten gegevens van iemand verzamelt, zeker als het gevoelige gegevens betreft (bijvoorbeeld over gezondheid). Een zorgvuldige omgang met de gegevens van burgers vormt een essentiële bouwsteen voor het vertrouwen van burgers in de overheid.

De gemeente Heemskerk heeft als wettelijke verplichting dat zij behoorlijk en zorgvuldig omgaat met (persoons-)gegevens om de persoonlijke levenssfeer, de privacy, van betrokkenen te beschermen. Bescherming van (persoons-)gegevens is een grondrecht; het juridisch kader is nationaal opgenomen in de Grondwet en is verder uitgewerkt in de Wet bescherming persoonsgegevens (Wbp). Lokaal geldt tevens de Gedragscode medewerkers gemeente Heemskerk (2009) en Gedragscode politieke ambtsdragers 2012.
De Wbp stamt echter nog uit de tijd toen zaken vooral alleen ‘op papier’ stonden. Met de inwerkingtreding van de Europese privacy-verordening, de Algemene Verordening Gegevensbescherming (AVG), is een vernieuwd en aangescherpt juridisch kader gekomen dat beter aansluit bij de hedendaagse praktijk. Overheden hebben tot 25 mei 2018 de tijd gekregen om te voldoen aan de bepalingen van de AVG.

Bij beleid op het gebied van gegevensbescherming gaat het echter niet enkel om naleving van de wet. Er zijn meer redenen waarom het vaststellen van overkoepelend privacy-beleid zo belangrijk is. Technologische ontwikkelingen gaan razendsnel. Voor de wetgever (nationaal en Europees) is het in feite niet mogelijk de ontwikkelingen bij te houden. Om binnen de organisatie te bepalen hoe met een bepaalde nieuwe ontwikkeling, vanuit privacy-oogpunt, moet worden omgegaan, is het bijzonder nuttig om overkoepelend beleid te hebben dat richting geeft aan de te maken keuzes. Het beleid helpt de organisatie regie te nemen in privacy-kwesties en, bij de verantwoording door het college in privacy-aangelegenheden, is het een belangrijk richtsnoer.

Dit beleid stelt de algemene kaders vast waarbinnen de gemeente bescherming van de gegevens van de burger regelt. Het geeft richting en kaders voor nader vast te stellen thematisch beleid (bijvoorbeeld op het gebied van personeel en organisatie). Daarnaast is het beleid bedoeld om het privacy-bewustzijn binnen de organisatie een ‘boost’ te geven en een open én kritische cultuur op het gebied van gegevensbescherming te creëren.

Het overkoepelend beleid Privacy & gegevensbescherming is IJmondiaal afgestemd. Beverwijk, Heemskerk en Velsen zijn zich er namelijk van bewust dat het meerwaarde biedt om de opgaven die er liggen in overeenstemming op te pakken en gelijkluidend uit te dragen.

1 Uitgangspunten

Dit beleid is van toepassing op alle verwerkingen van persoonsgegevens die plaatsvinden binnen de bureaus en bestuursorganen van gemeente Heemskerk en die vallen onder de werkingssfeer van de wet. Afscherming, corrigeerbaarheid en transparantie zijn de beleidsuitgangspunten waarmee het kader wordt geschetst en waarbinnen privacy-beleid wordt gevoerd.

1.1 Afscherming

Afscherming zorgt ervoor dat persoonsgegevens niet op een onrechtmatige manier kunnen worden verwerkt, zoals het gebruiken, doorgeven of koppelen van persoonsgegevens voor andere doelen dan de oorspronkelijke of voor onbekende doeleinden.

Doelbinding

Persoonsgegevens worden alleen verzameld en verwerkt voor vooraf welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en worden niet verder verwerkt voor andere doelen die hiermee onverenigbaar zijn (proportionaliteit en subsidiariteit).
Zo is er bijv. in de praktijk vaak een belangrijk verschil tussen 'dat informatie' (bv. gegeven dát iemand een strafblad heeft) en 'wat informatie' (wát er uit blijkt). Vanuit proportionaliteit is het dan steeds nodig aftewegen of er alleen 'dat' informatie, of ook 'wat' informatie moet worden gedeeld.

Noodzakelijkheid en limitering van verzamelen en gebruik van gegevens

De verzameling en verwerking van persoonsgegevens is toegespitst op een gespecificeerd doel met een wettelijke grondslag. Minimalistisch gegevensgebruik is het uitgangspunt (data-minimalisatie). Identificatie en traceerbaarheid van de betrokkene duurt niet langer dan strikt noodzakelijk is om het doel te bereiken.
Geautomatiseerde verwerking van persoonsgegevens met als doel de betrokkene te evalueren, te classificeren of een beslissing over die betrokkene te nemen, dit door persoonsgegevens te vergelijken en samen te brengen is alleen toegestaan met expliciete toestemming. (profilering)
Persoonsgegevens worden nooit verzameld, omdat dat later 'handig' kan blijken te zijn.

Bewaren

Persoonsgegevens worden niet langer bewaard dan voor het bereiken van het gespecificeerde doel noodzakelijk is, tenzij dit op basis van wetgeving (bijv. de Archiefwet) verplicht is.

Beveiligen

Op basis van de Baseline Informatiebeveiliging Gemeenten (BIG) worden passende technische en organisatorische beveiligingsmaatregelen genomen tegen elke vorm van onrechtmatige verwerking van persoonsgegevens, waaronder verlies of vernietiging van de gegevens, onrechtmatige toegang, gebruik, wijziging of openbaarmaking van gegevens. Daarbij wordt rekening gehouden met de stand van de techniek en de kosten van de implementatie van de beveiligingsmaatregelen.

Bij de inrichting van een werkproces - inclusief de ICT infrastructuur – wordt er vooraf nagedacht (privacy by design) over welke vragen en problemen vanuit privacy-oogpunt een rol (kunnen) spelen. Gebeurt dat, en worden daarbij goede oplossingen bedacht en ingeregeld, dan wordt er aan de voorkant voor gezorgd dat bepaalde privacy-problemen zich niet kúnnen voordoen.

Doorgifte naar derden

Persoonsgegevens worden slechts naar derden doorgegeven wanneer is vastgelegd en bekrachtigd dat aan alle wettelijke eisen wordt voldaan. Bij verwerking van persoonsgegevens door een bewerker wordt er een bewerkersovereenkomst afgesloten.
Aanvullend wordt voor doorgifte naar een land buiten de Europese Unie (EU) en de Europese Economische Ruimte (EER) alleen doorgegeven indien dat land een passend privacy beschermingsniveau waarborgt.

1.2 Corrigeerbaarheid

Tijdens en na elke verwerking van persoonsgegevens is het mogelijk om de persoonsgegevens en de uitkomsten van de verwerking te corrigeren, indien deze niet voldoen aan de doelbinding of de kwaliteitsvereisten en daardoor de betrokkene (kunnen) benadelen.

Kwaliteit

Gegevens zijn steeds voldoende actueel en zijn een nauwkeurige weergave van de feitelijke situatie. Het verwerken van onjuiste gegevens kan tot grote problemen leiden, met vervelende gevolgen voor de betrokkene en voor de goede uitoefening van de overheidsfunctie. Daarom moeten alle redelijke maatregelen worden genomen om onjuiste persoonsgegevens direct te wissen en te rectificeren. Voor zover mogelijk, moeten er ook geautomatiseerd controles op bestanden met persoonsgegevens plaatsvinden.

1.3 Transparantie

Voor, tijdens en na de elke verwerking van persoonsgegevens is duidelijkheid over de doelbinding, de wettelijke grondslag en de organisatorische en technische inrichting van verwerking van de persoonsgegevens.

Accountability

De gemeente is (eind)verantwoordelijk voor de gegevensverwerking en de bescherming daarvan. Dit geldt ook als gegevens ter beschikking worden gesteld aan derden of worden gedeeld in samenwerkingsverbanden.

Rechten van betrokkenen

Betrokkenen worden geïnformeerd over het beleid over en het gebruik van hun persoonsgegevens in samenhang met de gebruikte technologie en kunnen daarover controle uitoefenen.
Het recht op inzage, informatie, correctie en verwijdering van gegevens is vertaald in laagdrempelige procedures en wordt helder gecommuniceerd richting betrokkenen.
Betrokkenen hebben het recht om hun persoonsgegevens, die zij hebben verstrekt, in een gestructureerde, gangbare en machine leesbare vorm te verkrijgen, en deze gegevens aan een andere verwerkingsverantwoordelijke over te dragen (dataportabiliteit)
Meldingen en klachten met betrekking tot privacy aspecten komen binnen bij de gemeente via de bestaande kanalen.
Bij datalekken worden de betrokkenen geïnformeerd als deze inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

2 Organieke inbedding

De wijze van verankering van het privacy-beleid binnen de gemeente vormt het fundament van de borging van dit belangrijke thema. Volgens privacywetgeving is het college van Burgemeester en Wethouders verantwoordelijk voor de juiste uitvoering van de wet. Dit hoofdstuk geeft aan op welke wijze de taken, verantwoordelijkheden en de borging van het beleid wordt georganiseerd binnen de gemeente.

2.1 Governance

Het college van Burgemeester en Wethouders

Het college is verantwoordelijk voor de juiste uitvoering van het privacy-beleid.

Voor onafhankelijk toezicht op de uitvoering van het privacy-beleid wijst het college een functionaris voor de gegevensbescherming aan.

Het college stelt het gemeentelijk privacy-beleid vast met inachtneming van de aanbevelingen van de functionaris voor de gegevensbescherming en bevordert de beschikbaarheid van voldoende middelen om privacybescherming passend te waarborgen.

Het college wijst uit haar midden een portefeuillehouder privacy & gegevensbescherming aan die bestuurlijk verantwoordelijk is voor de uitvoering van het gemeentelijk privacy-beleid en voor controle op de naleving van afspraken. De feitelijke uitvoering wordt opgedragen aan de functionaris voor de gegevensbescherming.
De portefeuillehouder privacy & gegevensbescherming ziet toe op de ontwikkeling en uitvoering van themagericht privacy-beleid (themabeleid).

Het bureauhoofd

Het bureauhoofd is verantwoordelijk voor de zorgvuldige verwerking van persoonsgegevens die binnen zijn of haar afdeling plaatsvindt. Indien de verwerking een bureau overstijgend karakter heeft en betrekking heeft op twee of meer bureaus ligt de verantwoordelijkheid bij de betreffende proceseigenaar.

Het bureauhoofd is verantwoordelijk voor de uitvoering van themabeleid binnen en conform de door het college gestelde kaders. Hierbij wordt bij voorkeur gebruik gemaakt van bestaande oplossingen, voor zover uit toetsing blijkt dat deze inpasbaar zijn.
Het bureauhoofd krijgt hiervoor ondersteuning van de functionaris voor de gegevensbescherming.

Het bureauhoofd draagt binnen zijn bureau zorg voor de inventarisatie van de risico's die samenhangen met de verwerkingen van persoonsgegevens en de naar aanleiding daarvan vereiste maatregelen. Hij stelt de functionaris voor de gegevensbescherming en het college hiervan op de hoogte.

Het bureauhoofd meldt een (wijziging of beëindiging van een) verwerking ten behoeve van opname in het register van de verwerkingsactiviteiten[1], evenals het beoordelen hiervan, bij de functionaris voor de gegevensbescherming.

Het bureauhoofd informeert de functionaris voor de gegevensbescherming over ontwikkelingen die relevant zijn voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens.

[1] Zie 2.3: Register van verwerkingsactiviteiten

Het bureauhoofd ziet erop toe dat gegevensbescherming een onderdeel van het werkoverleg is. Op deze wijze werkt de gemeente actief aan een open cultuur, het optimaliseren van kennis en een transparante procesuitvoering.

De functionaris voor de gegevensbescherming
De functionaris voor de gegevensbescherming coördineert, beheert en houdt toezicht op het gemeentelijk privacy-beleid en doet verslag aan het management en het college over de voortgang en de kwaliteit van de uitvoering van het gemeentelijke privacy-beleid en doet aanbevelingen die strekken tot verdere optimalisering.

De functionaris voor de gegevensbescherming verzorgt, namens het college, een tweejaarlijkse evaluatie van de uitvoering van het privacy-beleid en informeert de raad over de risico's en over de getroffen beheersmaatregelen binnen de processen waarvoor de gemeente verantwoordelijk is.

De functionaris voor de gegevensbescherming houdt een register bij van de verschillende meldingplichtige gegevensverwerkingen (register van de verwerkingsactiviteiten) en de door de gemeente gesloten bewerkersovereenkomsten, convenanten en privacy-protocollen.

De functionaris voor de gegevensbescherming adviseert en informeert de medewerkers en het college over ontwikkelingen die relevant zijn voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens, in specifieke kwesties of bij de totstandkoming van nieuw beleid of wet- en regelgeving.

De functionaris voor de gegevensbescherming initieert het opstellen van themabeleid en werkt deze, in overleg met het bureauhoofd en onder diens verantwoordelijkheid, uit.

De functionaris voor de gegevensbescherming heeft eigen bevoegdheden, conform art 38 en 39 van de AVG, om te toetsen of de aanwezigheid en de werking van het privacy-beleid afdoende binnen de gemeente is ingericht. Hij heeft vrij toegang tot systemen en processen van de gemeente.
De functionaris voor de gegevensbescherming kan ambtshalve een onderzoek instellen naar de wijze waarop de verwerking van persoonsgegevens plaatsvindt.

De functionaris voor de gegevensbescherming ziet, samen met de interne controller, toe op totstandkoming van een privacy auditplan op basis van uitgevoerde gegevensbeschermingseffect-beoordelingen. Hier worden ook de ijkpunten van de gekozen beheersmaatregelen volgens het themabeleid meegenomen.

De functionaris voor de gegevensbescherming treedt op als aanspreekpunt voor de burger bij de uitoefening van de privacy-rechten en de uitvoering van het privacy-beleid.

De functionaris voor de gegevensbescherming doet meldingen bij de toezichthoudende autoriteit, de Autoriteit Persoonsgegevens (AP).

De functionaris voor de gegevensbescherming organiseert activiteiten die een voortdurende bewustwording ten aanzien van privacy en gegevensbescherming ten doel hebben.

2.2 Themabeleid

Het themabeleid (onder andere op het gebied van het sociaal domein, burgerzaken, openbare orde en veiligheid en personeelszaken) beschrijft de visie op zorgvuldige verwerking van persoonsgegevens, de kaders waarbinnen gegevensverwerking plaatsvindt, de inhoudelijke beleidskeuzes (waaronder mate van integraliteit, doel gemeenten en gegevensverwerking, kwaliteitsmanagement, beveiliging en doorgifte van persoonsgegevens) in relatie tot de relevante (nieuwe) wettelijke kaders en de wettelijke kaders voor het verwerken, beheren en delen van gegevens binnen de diverse beleidsvelden.

Wanneer er wordt samengewerkt met externe partijen of activiteiten worden uitbesteedt waar persoonsgegevens in verwerkt worden, moet formeel afgestemd worden op welke manier de partijen met deze gegevens om dienen te gaan. Dit staat beschreven in convenanten en/of bewerkersovereenkomsten.

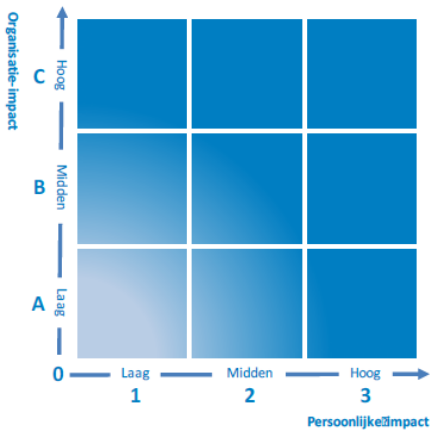
De uitgangspunten die beschreven staan in dit overkoepelend beleid komen terug of moeten praktisch worden vertaald in de werkprocessen waarin persoonsgegevens verwerkt worden. Daarnaast is het van belang dat er in de werkprocessen wordt nagedacht over de rollen en verantwoordelijkheden met betrekking tot de verwerking van persoonsgegevens, zoals welke personen welke gegevens mogen inzien om hun taak te kunnen uitvoeren (bv. autorisaties binnen systemen).

Het themabeleid wordt minstens eenmaal per vier jaar geëvalueerd.

2.3 Register van verwerkingsactiviteiten

Naast het belang van een overzicht van de gegevensverwerkingen en bewerkersovereenkomsten, is het belangrijk om te weten welke persoonsgegevens in welk systeem worden opgeslagen, hoe lang ze bewaard mogen of moeten worden en wat er na die termijnen mee gebeurd; welke informatie tussen systemen wordt uitgewisseld en welke beveiligingseisen er aan de systemen gesteld worden. Het register van verwerkingsactiviteiten is er ook om inzichtelijk te maken en te houden wie welke autorisatie heeft om persoonsgegevens te mogen verwerken, daarbij rekening houdend met de specifieke taak, rol en verantwoordelijkheid van de gebruiker of professional. In de bijlage staan de verdere vereiste gegevens welke opgenomen dienen te zijn in het register.

2.4 Privacy-risicomanagement



Privacy-risicomanagement is een continu proces dat de privacy-risico's signaleert, beoordeelt en het verkleinen ervan bewaakt.
Privacy-risicomanagement richt zich op het beheersen van privacy-risico's bij het verzamelen, verwerken, opslag en doorgeven van persoonsgegevens. Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen wordt vóór de verwerking een beoordeling uitgevoerd van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.
Door middel van deze gegevensbeschermingseffect-beoordelingen, ook wel Privacy Impact Assessments (PIA's) genoemd, worden bij de ontwikkeling en de inrichting van de organisatie, de privacy-risico's in lijn gebracht met het privacy-beleid. Zodoende wordt er voldaan aan de wet- en regelgeving en het belang van zowel de betrokkene als de organisatie wordt geborgd.

De risico’s worden door praktische, organisatorische en technische maatregelen beheerst. De effecten, zowel profijt als risico’s voor betrokkenen en de gemeente, zijn in kaart gebracht en zijn afgewogen op basis van de inhoud. Deze vormt het vertrekpunt voor het maken van beleidskeuzes.

Planning en control cyclus

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

2.5 Bewustwording en communicatie

Naast het inrichten van het privacy-beleid en werkprocessen is het van belang dat de personen die daadwerkelijk werken met deze gegevens weten wat hun verantwoordelijkheid is en hoe ze zorgvuldig om moeten gaan met persoonsgegevens. Daarom is het belangrijk dat de professionals in het veld en binnen de gemeente zich bewust zijn van de regels en gedragsnormen rondom gegevensbescherming. De gemeente zal dit proces ondersteunen door het ontwikkelen van bijv. praktische handleidingen en workshops.
De gemeente streeft een cultuur na waarbij professionals elkaar in alle openheid aanspreken op het eigen gedrag rondom privacy en daarmee van elkaar leren. Communicatie, openheid en toetsing zijn belangrijke randvoorwaarden voor het realiseren van een optimale inbedding van het privacy-beleid.

Richting de burger is communicatie over gegevensbescherming van belang. De burger heeft het recht te weten wat er met zijn of haar gegevens gebeurt. De burger zal actief geïnformeerd worden over het privacy-beleid via website en andere kanalen. Het gaat hierbij niet alleen om informatie over de manier waarop de gemeente met persoonsgegevens omgaat maar ook om informatie over de rechten van burgers, zoals inzage- en correctierecht van gegevens, de mogelijkheid verzet aan te tekenen tegen verwerking en het vernietigingsrecht als wel informatie over de bezwaar- en klachtenprocedure.

2.6 Evaluatie

Het privacy-beleid is geen statisch document en zal op termijn geëvalueerd moeten worden in samenspraak met de IJmond gemeenten, waarbij veranderde inzichten, wettelijke wijzigingen en best practices meegenomen worden.

Bijlage: Register van werkingsactiviteiten

Bij de inschrijving worden, minstens, de volgende gegevens vermeld:

- de verantwoordelijke;
- de naam van de verwerking;
- het betreffende bureau en cluster;
- de doeleinden van de verwerking;
- de gronden van de verwerking;
- de herkomst/verkrijgingswijze van de persoonsgegevens;
- de personen van wie persoonsgegevens worden verwerkt (betrokkenen);
- de persoonsgegevens die worden verwerkt;
- de ontvangers aan wie de gegevens kunnen worden verstrekt;
- de bewaartermijn van de gegevens;
- een algemene omschrijving van de beveiligingsmaatregelen;
- indien van toepassing, doorgifte aan landen buiten de EU;
- indien van toepassing, de bewerker;
- het meldingsnummer bij het AP dan wel de vrijstellingsgrond;
- eventuele bijzonderheden.

Bij wijziging van een of meer van de genoemde gegevens wordt de verwerking in het register van de verwerkingsactiviteiten aangepast.
Bij beëindiging van een verwerking wordt de verwerking in het register van de verwerkingsactiviteiten doorgehaald.