Gemeente Heerde

cittaslow









2019

Jaarrapportage gegevensbescherming

www.heerde.nl

Samenvatting

Het jaar 2019 was op het gebied van gegevensbescherming een bijzonder jaar voor organisaties en inwoners, zo ook voor de gemeente Heerde. Op 25 mei 2018 het jaar daarvoor werd namelijk de Algemene Verordening Gegevensbescherming (AVG) van kracht en in 2019 kreeg deze wetgeving verdere aandacht.

De AVG verving de Wet bescherming persoonsgegevens (Wbp) en zorgt voor een verhoogde aandacht voor een rechtmatige verwerking van persoonsgegevens in alle sectoren. Tevens is er een verhoogd boeteregime ontstaan. Voor het niet voldoen aan de AVG kan een maximale boete worden opgelegd van €20.000.000,- of 4% van de wereldwijde omzet. De (lokale) overheid heeft bovendien een belangrijke voorbeeldfunctie voor wat betreft het naleven van de AVG.

Het college van B&W is als bestuursorgaan verantwoordelijk voor het merendeel van de verwerkingen van persoonsgegevens in onze gemeente. Dit brengt verplichtingen met zich mee. In deze jaarrapportage staat beschreven welke acties en maatregelen de gemeente Heerde in 2019 heeft genomen om de doelstellingen en beginselen uit de AVG te behalen en te waarborgen.

Ook bevat dit document aandachtspunten en actiepunten voor het jaar 2020. Adequaat omgaan met persoonsgegevens is een blijvend proces en zal dan ook aandacht blijven vergen van zowel bestuur, management als medewerkers.

Samenvattend heeft de gemeente in 2019 veel werk verzet op het gebied van gegevensbescherming. Zo is onder andere nadere invulling gegeven aan de organisatorische inbedding van gegevensbescherming door het aanstellen van een tijdelijke parttime Privacy Officer (PO), Chief Information Security Officer (CISO) en een nauwe samenwerking aan te gaan met de gemeente

Hattem en Oldebroek.[1] Tevens is er gewerkt aan het opstellen van een zogenaamd 'verwerkingsregister', één van de vereisten vanuit de AVG, en zijn er allerlei privacyvraagstukken vanuit de organisatie behandeld.

Hieronder volgt een algemeen beeld met bevindingen en aanbevelingen omtrent de mate van gegevensbescherming binnen de gemeente Heerde.

AVG thema's	Bevindingen en aanbevelingen
Privacybeleid Een privacybeleid is met de AVG een wettelijke verplichting geworden. Hierin staat beschreven hoe de gemeente omgaat met privacy en invulling geeft aan de AVG.	In 2018 is een privacybeleid vastgesteld. Dit dient jaarlijks te worden geactualiseerd en uitgedragen te worden binnen de gemeente. Gebleken is dat veel medewerkers nog onbekend zijn met het beleid. Aan te raden is dat het privacybeleid wordt geactualiseerd in samenwerking met Oldebroek en Hattem, aangezien daarmee intensief wordt samengewerkt op dit vlak. Tevens dient aandacht te worden gegeven aan het bestaan en de inhoud van het beleid bij medewerkers.
Processen Processen binnen de gemeente waarbij persoonsgegevens worden gebruikt dienen te voldoen aan de beginselen vanuit de AVG.	In 2019 bezat de gemeente Heerde geen actueel overzicht van alle processen met persoonsgegevens die zij uitvoert. Hierdoor is onduidelijk in hoeverre alle aanwezige processen voldoen aan de AVG. De gemeente dient een duidelijk overzicht te hebben van deze processen zodat een structurele controle hierop kan plaatsvinden. Tevens dienen medewerkers zich ervan bewust te zijn dat zij verantwoordelijk zijn voor de processen die onder hen plaatsvinden inclusief de mate waarin deze aan de AVG-beginselen voldoen.
Gegevensbeschermingseffect-beoordeling (DPIA) De DPIA is een voorgeschreven middel vanuit de AVG waarmee processen van te voren kunnen worden beoordeeld op de privacy-impact voor betrokkenen. In sommige situaties waarbij een hoog privacy-risico aanwezig is, is een DPIA wettelijk verplicht. Bijv. bij de toepassing van zgn. Smart-City applicaties of het inzetten van cameratoezicht.	In 2019 heeft de gemeente Heerde onderzocht op welke wijze DPIA's optimaal kunnen worden uitgevoerd. De gemeente heeft in 2019 zelf nog geen DPIA's uitgevoerd. Het uitvoeren van een DPIA dient een reguliere aangelegenheid te worden en onderdeel van de voorbereidingsfase bij projecten, processen en aankoop van ondersteunende applicaties waarbij persoonsgegevens worden gebruikt. Hiervoor is het van belang dat het gehele proces omtrent de uitvoering van een DPIA wordt beschreven en kenbaar wordt gemaakt binnen de organisatie.

[1] Een Privacy Officer (PO) is een medewerker van de gemeente aangesteld om met name de uitvoerende aspecten van gegevensbescherming te behandelen, op casus niveau advies te geven over de juiste toepassing van gegevensbescherming binnen de organisatie en dit aan te jagen. De Chief Information Security Officer (CISO) is een adviseur en deskundige op het vlak van het identificeren, voorkomen en verminderen van (technische) IT-beveiligingsrisico's.

Organisatorische inbedding Organisatorische inbedding betekent hier het toewijzen van rollen en taken, verantwoordelijkheden en bevoegdheden en het creëren van bewustzijn.	Afgelopen jaar is er met de aanstelling van de tijdelijke PO en CISO een professionalisering gemaakt op het gebied van informatiebeveiliging & privacy. Ook zijn er stappen gemaakt in het verhogen van de bewustwording onder medewerkers o.a. d.m.v. een e-learning en het toegankelijk maken van bruikbare informatie via intranet. Het is aan te bevelen dat deze tijdelijke rollen z.s.m. permanent worden ingevuld. Daarnaast is het aan te bevelen dat er binnen de afdelingen medewerkers worden aangewezen die privacy-gerelateerde werkzaamheden voor hun afdeling kunnen uitvoeren (bijv. als zgn. privacy-ambassadeurs).
Rechten van betrokkenen De gemeente dient betrokkenen te informeren over de wijze waarop zij omgaat met hun persoonsgegevens. Daarnaast stelt de AVG betrokkenen in staat om middels een aantal rechten controle en invloed uit te oefenen over zijn of haar persoonsgegevens.	De gemeente Heerde heeft het afgelopen jaar een privacyverklaring beschikbaar gesteld waarmee inwoners inzicht krijgen in de wijze waarop de gemeente persoonsgegevens verwerkt. Ook zijn er procedures ingesteld waarmee inwoners gebruik kunnen maken van hun AVG-rechten. Tot op heden is hier slechts eenmaal gebruik van gemaakt. Bij domeinen waar gevoelige informatie, zoals het sociale domein, wordt verwerkt dient extra aandacht worden besteedt aan het voorzien van de juiste informatie aan betrokkenen. Dit kan bijv. in de vorm van brochures. Daarnaast dienen medewerkers te worden gewezen op hun rol bij procedures waarmee betrokkenen gebruik kunnen maken van hun AVG-rechten.
Samenwerking Onder de AVG is de gemeente verplicht om afspraken te maken met derde partijen als hiermee persoonsgegevens worden uitgewisseld.	De gemeente Heerde heeft het afgelopen jaar met meerdere partijen de nodige afspraken gemaakt omtrent gegevensbescherming. Er is echter nog onvoldoende zicht op in hoeverre er met alle betreffende partijen de nodige afspraken zijn gemaakt. De gemeente dient over een actueel overzicht te beschikken van partijen waarmee afspraken moeten worden gemaakt op het gebied van gegevensbescherming. Tevens dient aandacht te worden gegeven aan contractmanagement.
Beveiliging De gemeente Heerde is onder de AVG verplicht passende technische en organisatorische beveiligingsmaatregelen te nemen. Tevens geldt er onder de AVG een meldplicht datalekken die inhoudt dat bepaalde datalekken aan de Autoriteit Persoonsgegevens (AP) en betrokkenen dienen te worden gemeld.	In 2019 is er een datalekprotocol binnen de gemeente Heerde vastgesteld en een meldingsformulier beschikbaar gesteld op intranet. Hiermee kunnen medewerkers datalekken tijdig melden. In 2019 zijn er in totaal 10 datalekken gemeld binnen de gemeente Heerde. Van deze 10 zijn er 7 gemeld bij de AP. In 1 van de 10 gevallen zijn de betrokkenen hierover geïnformeerd. Er dient blijvend aandacht te worden gegeven aan het risico dat datalekken met zich meebrengen voor de organisatie alsook voor betrokkenen.

Verantwoordingsplicht Onder de AVG dienen organisaties zelf aantoonbaar te maken dat zij compliant zijn. Onderdeel hiervan is het verplichte verwerkingsregister. Hierin staan alle processen opgenomen waarbij persoonsgegevens worden verwerkt. Per proces wordt o.a. aangegeven wat het doel is, welke persoonsgegevens worden gebruikt etc.	De gemeente Heerde heeft in 2019 gewerkt aan het opstellen van het verwerkingsregister. Inmiddels staan hier een groot aantal processen in opgenomen. In 2020 dient hier verder aan te worden gewerkt en dient dit belegd te worden in de lijn. Het register kan hierdoor een belangrijk brondocument worden waarmee gegevensbescherming binnen de organisatie geborgd wordt.