Gemeente Zeist

GEMEENTEBLAD

Officiële uitgave van de gemeente Zeist

Nr. 91199

16 april

2019

Besluit van het college van burgemeester en wethouders van de gemeente Zeist houdende regels omtrent privacy beleid gemeente Zeist

Inleiding

Voor het uitvoeren van de gemeentelijke taken verwerkt en bewaart gemeente Zeist persoonsgegevens van haar inwoners, andere klanten en (keten)partners. De mensen op wie deze persoonsgegevens betrekking hebben (betrokkenen), moeten erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met hun persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering, toename in het verzamelen en delen van gegevens, cybercrime en een steeds meer digitale overheid stellen andere en hogere eisen aan de bescherming van gegevens en aan privacy.
Privacy speelt een steeds belangrijkere rol in de relatie tussen de burger en de overheid. Wij vinden deze relatie belangrijk, want willen een betrouwbare overheid zijn, en dus willen wij zo goed mogelijk de privacy van onze relaties waarborgen.
Als gemeentelijke organisatie zijn wij wettelijk verplicht om zorgvuldig, veilig en vertrouwelijk om te gaan met het verzamelen, bewaren en beheren van persoonsgegevens. Dat geldt voor taken op alle terreinen waarop de gemeente taken uitvoert, maar zeker voor bijvoorbeeld het bijhouden van de Basisregistratie Persoonsgegevens (BRP), het bewaken van de openbare orde en veiligheid en het uitvoeren van de wetten in het sociaal domein.

Privacy vraagt niet alleen om een heldere bestuurlijke visie op privacy (zie visie op privacy uit 2016) maar ook om duidelijke beleidskaders. Deze notitie verwoordt de visie op privacy zoals deze besloten ligt in de Nederlandse en Europese wetgeving.
Privacywetgeving is geen *'kan niet / mag niet-wetgeving'* maar schept juist ruimte. Daarvoor is een aanpak nodig die erg lijkt op risicomanagement, een aanpak van *'Pas toe of leg uit*. Hoewel er ook verschillen zijn omdat privacy uiteindelijk een integriteitsaangelegenheid is (moraliteit). Het invoeren van privacy beleid is niet zozeer een extra last maar geeft de gemeente de mogelijkheid om uiting te kunnen geven aan de eigen bestuurlijke visie en dus de manier waarop ze met haar inwoners en ketenpartners om willen gaan.

1. Hoe borgt gemeente Zeist de bescherming van de privacy?

De gemeente heeft al enige jaren een gemeente breed Informatieveiligheidsbeleid. Dit beleid heeft betrekking op de borging van de veiligheid van informatievoorziening in zijn algemeenheid.
Een betrouwbare informatievoorziening is tenslotte noodzakelijk voor het goed functioneren van de gemeente en vormt de basis voor het beschermen van rechten van burgers en bedrijven [1]. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn waarbij ieder organisatieonderdeel en met name het bestuur is j betrokken. Het niet of onvoldoende borgen van informatieveiligheid en privacy levert risico's op. Dit kan leiden tot imagoschade, politieke schade en financiële schade door de boetes die kunnen worden opgelegd.

Voor dit beleid is de landelijke Baseline Informatiebeveiliging Gemeenten (BIG) gevolgd, waarmee gemeenten op een vergelijkbare manier aan alle eisen op het gebied van informatiebeveiliging kunnen voldoen. Er is een bestaand gemeente breed Informatieveiligheidsbeleid "Weerbaar en Bewust 2016-2018) dat is te raadplegen op onze website [2]:
Zoals hiervoor gezegd is het Informatieveiligheidsbeleid veel breder dan privacybescherming alleen. Wij vinden het belangrijk om daarnaast een document te hebben dat zich speciaal op privacybescherming richt. Wij willen dat onze relaties (en zeker onze inwoners) op een toegankelijke wijze geïnformeerd worden over hoe wij omgaan met hun wettelijk beschermde privacy rechten. Met dit document leggen wij verantwoording af over hoe wij met persoonsgegevens omgaan en zijn wij daarop ook aanspreekbaar.

1) *Met betrouwbaarheid wordt bedoeld: beschikbaarheid (continuïteit van de bedrijfsvoering), 'integriteit (juistheid, volledigheid) en 'vertrouwelijkheid (geautoriseerd gebruik) van gegevens en informatie.*

2) *https://www.zeist.nl/fileadmin/bestanden/Documenten/Gemeentebestuur/BeleidInformatieveiligheid_2016-2018_Weerbaar_en_Bewust.pdf]*

Gemeente brede visie op Privacy
Privacy is onlosmakelijk verbonden met het thema Informatieveiligheid. Vanuit die optiek was het logisch om ook een visie op privacy te formuleren waarbij elementen zoals wetgeving, kernwaarden en hoe we dit concreet willen vertalen in onze dienstverlening verwerkt zijn. Daarom is al in 2006 de visie op privacy vastgesteld. *Privacy en de kunst van het selectief verzamelen (De balans tussen afstand en nabijheid)*[3]

Uitgangspunten voor deze visie en de uitwerking daarvan waren onder andere de kernwaarden: vertrouwen, nabijheid en kracht en de Brede Sociale Visie (BSV). Dit vraagt om een omgang met privacy op maat waarbij telkens opnieuw afwegingen worden gemaakt en waarbij gezocht wordt naar het juiste evenwicht. Leidend daarbij is dat de gemeente niet meer gegevens verzamelt en vastlegt dan nodig is, niet meer mensen toegang geeft tot deze gegevens dan nodig is en dat de gemeente open is over wat er met deze gegevens gebeurt, zodat de gemeente zich te allen tijde een betrouwbare partner toont.

Visie op privacy: Door precies die beperkte hoeveelheid informatie te verzamelen en te gebruiken die nodig is voor de taakuitoefening en dit steeds te toetsen, zijn we als overheid een betrouwbare partner. Door niet uit te gaan van risicomijding maar professionaliteit werken we vanuit ieders kracht.
Deze visie op privacy gebruiken we als kapstok om diverse uitvoeringszaken zoals privacy reglementen, bewerkingsovereenkomsten, de samenwerking in de regio, maar ook de diverse administraties vorm te geven.

Nieuwe privacywetgeving
Na de vaststelling van het Informatieveiligheidsbeleid is in 2016 de Europese Algemene Verordening Gegevensbescherming gekomen, die in Nederland op 25 mei 2018 in werking is getreden onder de naam AVG. Deze verordening vervangt onze nationale Wet bescherming persoonsgegevens en scherpt die verder aan. De AVG vraagt van ons als verwerkingsverantwoordelijke, transparantie en verantwoording over de naleving van de eisen die in de AVG aan ons worden gesteld. Mede door dit document willen wij aan die eisen voldoen.

2. Begrippen

De volgende begrippen zijn voor dit document van belang.

Persoonsgegevens: Alle informatie die gaat over een geïdentificeerde of identificeerbare persoon (de betrokkene). Het gaat hierbij om ieder gegeven dat te herleiden is tot een bepaald natuurlijk persoon. Er zijn gewone persoonsgegevens zoals naam, adres, woonplaats en bijzondere persoonsgegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren of het Burgerservicenummer (BSN).

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

Verwerker: De persoon of organisatie die de persoonsgegevens verwerkt.

Verwerking: Het verzamelen, vastleggen, raadplegen, gebruiken, verstrekken door middel van doorzending, of op andere wijze ter beschikking stellen, wijzigen, wissen.

Verwerkingsverantwoordelijke: Een persoon of instantie die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. De bestuursorganen van de gemeente zijn allemaal verwerkingsverantwoordelijken voor de verwerkingen die door of namens de gemeente worden uitgevoerd. De bestuursorganen van de gemeente zijn onder andere de burgemeester, het college van Burgemeesters en Wethouders (college van B&W) en de gemeenteraad.

Gegevensbeschermingseffect beoordeling: Met een gegevensbeschermingseffect beoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit heet ook wel een Data Privacy Impact Assessment (DPIA).

3) Visie op privacy: Privacy en de kunst van het selectief verzamelen (16cv-00338)

3. Reikwijdte privacy beleid

Het privacy beleid is van toepassing op de hele organisatie en alle processen waarbij persoonsgegevens worden gebruikt. Ook de processen van de raad en die van bestuurlijke (advies)commissies waarbij persoonsgegevens worden gebruikt vallen onder de reikwijdte van dit beleid.
Wat onder persoonsgegevens wordt verstaan, om wiens persoonsgegevens het gaat, hoe de gemeente er aan komt en wanneer de gemeente persoonsgegevens mag gebruiken wordt hieronder beschreven.
Het beleid geldt voor een ieder die namens de gemeente gebruik maakt van persoonsgegevens.
Onder gebruik wordt verstaan: verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, aan derden geven, verspreiden of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, en het afschermen, uitwissen of vernietigen van gegevens.
Het privacy beleid geldt als algemeen beleid. Hierin zijn de kaders, uitgangspunten, taken, verantwoordelijkheden en maatregelen beschreven om de persoonsgegevens te beschermen. Voor bepaalde domeinen kan het nodig zijn om aanvullend een specifiek privacy beleid vast te stellen.

Wat is een persoonsgegeven en hoe komen we eraan?
Het gaat om gegevens die direct of indirect informatie verschaffen over een natuurlijk persoon. Naam, geboortedatum, geslacht en adresgegevens zijn directe gegevens. Uiterlijke, sociale en economische kenmerken is indirecte informatie die in combinatie met andere gegevens kan leiden tot identificatie van een persoon.
De wet maakt onderscheid tussen gewone persoonsgegevens en bijzondere persoonsgegevens. Bijzondere persoonsgegevens zijn gegevens die gevoelige informatie over een persoon verschaffen, zoals gegevens over gezondheid of strafrechtelijke gegevens. Het gebruik van bijzondere persoonsgegevens is verboden, tenzij in de wet een uitzondering op dit verbod is opgenomen.
Persoonsgegevens worden zoveel mogelijk door de persoon zelf verstrekt. Soms zijn gegevens afkomstig van derden, zoals uitkeringsinstanties.

Van wie worden persoonsgegevens gebruikt, wanneer en waarom?
Van iedereen die gebruik maakt van de dienstverlening van de gemeente. En iedereen die werkzaam is voor de gemeente.
Binnen de gemeente gebruiken we persoonsgegevens echter alleen voor een bepaald doel. Het doel van het gebruik en de soort gegevens kunnen per product of dienst verschillen. Het doel kan zijn het afhandelen van aanvragen, heffen en innen van belastingen, verstrekken van uitkeringen of subsidies of betalen van huur voor een stukje grond. En we verzamelen en gebruiken daarbij verschillende soorten gegevens. Dit kunnen naam en adresgegevens zijn, maar soms ook gevoelige gegevens ofwel bijzondere persoonsgegevens zoals het BSN nummer of gezondheidsgegevens.
Persoonsgegevens mogen alleen worden gebruikt als daar een wettelijke basis voor is. Deze basis kan slechts zijn: uitvoeren van een overeenkomst, uitvoeren van een wettelijke verplichting, uitvoeren van een publieke taak, bij een vitaal belang, een gerechtvaardigd belang of met toestemming.

4. Wet- en regelgeving

Er is diverse wetgeving van toepassing op privacy:

De eerbiediging van de persoonlijke levenssfeer (privacy) is een grondrecht en onder meer geregeld in:
° artikel 8 van het Europese verdrag voor de rechten van de mens (EVRM)
° artikelen 7 en 8 Handvesten Grondrechten EU;
° artikel 10 Grondwet;

Bescherming van persoonsgegevens is een onderdeel van privacy in het algemeen en is geregeld in:
° de Algemene Verordening Gegevensbescherming (AVG) die vanaf 25 mei 2018 geldt;
° de Uitvoeringswet AVG.
°

Er zijn ook nog andere (materie)wetten die het gebruik van persoonsgegevens regelen en die, indien van toepassing, voorgaan op de Uitvoeringswet AVG, omdat zij specifieke regels bevatten op hun terrein. Te denken valt aan:
° de Wet basisregistratie personen (Wet BRP)

- de Wet politiegegevens;
- de Jeugdwet;
- de Wet maatschappelijke ondersteuning 2015.

De gemeente voert haar wettelijke taken vaak uit met anderen. Dit kan door taken uit te besteden aan derden of samen te werken met andere partijen. Met deze partijen worden schriftelijke afspraken gemaakt over de bescherming van persoonsgegevens. Deze afspraken worden vastgelegd in contracten (verwerkersovereenkomsten), in privacyreglementen of convenanten met samenwerkingspartners.

5. Uitgangspunten en beginselen

Gemeente Zeist handelt naar de volgende (wettelijke) beginselen ter bescherming van persoonsgegevens. Iedereen werkzaam binnen de organisatie is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacy rechten van personen Het gebruik van persoonsgegevens is rechtmatig, behoorlijk en transparant.
Het is constant zoeken naar een evenwichtige balans tussen bescherming persoonsgegevens, dienstverlening en werkbaarheid. Waar nodig en mogelijk wordt het advies en de deskundigheid van wetgever, toezichthouder of koepelorganisatie betrokken bij dilemma's:

a. *Transparantie en communicatie*
De gemeente wil aan betrokkenen duidelijke, beknopte en begrijpelijke informatie over de verwerking van zijn persoonsgegevens en van zijn rechten geven.

b. *Zorgvuldigheid, behoorlijkheid, juistheid*
Persoonsgegevens worden correct verwerkt en zijn betrouwbaar. Zij zullen in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt.

c. *Rechtmatigheid (grondslag en doel)*
Persoonsgegevens mogen alleen verwerkt worden als daarvoor een doel is vastgesteld. Voor elke verwerking van persoonsgegevens is een rechtmatige grondslag te geven.
Dat betekent dat de verwerking alleen mag plaatsvinden als aan ten minste één van de onderstaande voorwaarden is voldaan:

- Om een verplichting na te komen die in de wet staat
- Voor de uitvoering van een overeenkomst waarvan de betrokkene partij is
- Om een betrokkene te beschermen in een voor hem (levens)bedreigende situatie (bescherming van een vitaal belang)
- Voor de goede vervulling van een taak van algemeen belang of in het kader van de uitoefening van openbaar gezag dat aan de gemeente is opgedragen
- Als er geen wettelijke grondslag is te geven: als de betrokkene toestemming heeft gegeven voor de verwerking van persoonsgegevens voor één of meer specifieke doeleinden.

Als persoonsgegevens voor een hierboven genoemd doel zijn verzameld, mogen deze vervolgens niet zonder toestemming van de betrokkene voor andere doelen verwerkt worden.

d. *Noodzakelijk en proportioneel*
De gemeente mag alleen de persoonsgegevens verwerken die noodzakelijk zijn voor het vooraf bepaalde doel. Ook zullen de persoonsgegevens toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is voor het doel van verwerking.

d. *Bewaartermijn*
Persoonsgegevens mogen niet langer worden bewaard dan nodig is en wettelijk is voorgeschreven.

e. *Integriteit en vertrouwelijkheid*
De gemeente wil dat persoonsgegevens vertrouwelijk worden behandeld.

f. *Persoonsgegevens delen*
In het geval van samenwerking met externe partijen, waarbij sprake is van het uitwisselen van persoonsgegevens waarvoor de gemeente verantwoordelijk is en blijft, zal de gemeente ervoor zorgen dat die partij ook voldoet aan de wettelijke eisen ter bescherming van persoonsgegevens.

g. *Rechten van betrokkenen*
De betrokkenen hebben op grond van de wet rechten als hun persoonsgegevens worden verwerkt, zoals het inzagerecht, het recht op verbetering, correctie en verwijdering. De gemeente zal deze rechten waarborgen.

6. Van beginselen naar maatregelen

De gemeente moet passende organisatorische en technische maatregelen treffen om aan de beginselen ter bescherming van persoonsgegevens te voldoen. Aan de hand van de genoemde beginselen in hoofdstuk 5 bespreken wij hieronder welke maatregelen wij hebben getroffen. En kunt u lezen op welke manier wij uitvoering geven aan de beginselen voor de verwerking van persoonsgegevens in de praktijk. Met de maatregelen beschreven in dit hoofdstuk kunnen de privacy voorschriften worden nageleefd en de risico's worden beperkt. Het zijn wettelijke maatregelen om persoonsgegevens rechtmatig, behoorlijk en transparant te gebruiken. Door het treffen van deze maatregelen voldoet de gemeente aan haar verantwoordingsplicht.

6.1 Beginselen

Transparantie en communicatie
Om te voldoen aan dit beginsel zorgen wij ervoor dat betrokkenen bij het eerste contact waarbij persoonsgegevens worden vastgelegd, worden geïnformeerd over het doel en de rechtsgrond van de verwerking van de persoonsgegevens, de eventuele uitwisseling van deze gegevens, de termijn van bewaring en de rechten van betrokkenen. Dit gebeurt zowel schriftelijk als mondeling.
Wij zorgen ervoor dat er duidelijkheid bestaat over de wijze van de uitoefening van deze rechten. Voor de afhandeling van verzoeken van betrokkenen ter uitoefening van hun rechten worden interne protocollen en processen opgesteld. Ook worden daarvoor technische maatregelen in onze informatiesystemen getroffen.

Zorgvuldigheid, behoorlijkheid, juistheid
De gemeente zorgt ervoor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. Persoonsgegevens worden in eerste instantie opgevraagd uit authentieke bronnen zoals de Basisregistratie personen.

Rechtmatigheid (grondslag en doel, noodzaak en proportionaliteit)
Wij verwerken persoonsgegevens voor verschillende doelen ter uitvoering van diverse taken. Wij beschikken daarvoor over verschillende, van elkaar gescheiden informatiesystemen, zoals bijvoorbeeld de Basisregistratie personen, de Basisregistratie adressen en gebouwen, Zorgned voor de uitvoering van de Wet maatschappelijke ondersteuning en Jeugdwet en een zaaksysteem. In principe borgt het informatiesysteem zelf de bewaking van de doelbinding en de grondslag voor de gegevensverwerking. Als het doel en de grondslag toch onvoldoende blijken te zijn geborgd, dan nemen wij maatregelen om eventuele inbreuken op de privacy te voorkomen. Het is belangrijk dat medewerkers de rechtmatigheidsvoorwaarden ook echt toepassen en eventuele inbreuken signaleren. Wij blijven daarom scherp op de toepassing van de rechtmatigheidstoetsing voordat persoonsgegevens worden verwerkt. Zeker in het sociaal domein, waarbinnen veelal gevoelige persoonsgegevens omgaan, is daar extra aandacht voor.

Bijzondere categorieën van persoonsgegevens
Bijzondere persoonsgegevens zijn gegevens over ras, etnische afkomst, genetische, biometrische of gezondheidsgegevens of gegevens over seksuele gerichtheid. Ook het Burgerservicenummer en financiële gegevens zijn gevoelige persoonsgegevens die extra bescherming vereisen. Deze gegevens leggen wij in principe niet vast omdat deze gegevens dieper in de privacy sfeer van personen liggen. De noodzaak tot vastlegging daarvan ontbreekt dan ook in de meeste gevallen. Als die noodzaak wel aan de orde is, zoals vingerafdrukken bij het aanvragen van een identiteitsbewijs, dan worden deze, voor zover noodzakelijk en proportioneel, wel verwerkt. De noodzaak tot verwerking van deze gevoelige persoonsgegevens is alleen aanwezig als dit wettelijk is vastgelegd. Dit geldt bijvoorbeeld voor gezondheidsgegevens in de Jeugdwet en de Wet maatschappelijke ondersteuning, waar wij een belangrijke taak in hebben.

Integriteit en vertrouwelijkheid
Persoonsgegevens worden alleen verwerkt door personen die taken uitoefenen waarvoor de betreffende verwerking van persoonsgegevens noodzakelijk is. Medewerkers van de overheid hebben de wettelijke plicht tot geheimhouding van vertrouwelijke gegevens waarmee zij bij de uitoefening van hun taak in aanraking komen. Daartoe worden in principe alle persoonsgegevens gerekend. Deze geheimhoudingsplicht geldt uiteraard ook voor het college, de raad en de burgemeester.
Dit betekent ook dat persoonsgegevens niet intern worden gedeeld als dit niet noodzakelijk is. Collegiaal overleg met niet-behandelaars waarbij gevoelige persoonsgegevens over bijvoorbeeld gezondheidsaspecten ter sprake komen, gebeurt op casus niveau zonder vermelding van naam en adres van de betrokkene.

Rechten van betrokkenen
Iedereen heeft recht op informatie over de persoonsgegevens die de gemeente van hem of haar gebruikt en over het doel waarvoor de gegevens worden gebruikt, om deze in te zien en ook om deze gegevens te verbeteren, aan te vullen te verwijderen of af te schermen als deze feitelijk onjuist, onvolledig of niet relevant zijn. De gemeente communiceert actief over deze rechten op de gemeentelijke website en in andere uitingen.
Deze rechten zijn opgenomen in een document op de website onder het kopje privacy rechten. Als persoonsgegevens niet bij de betrokkene zelf worden verkregen dan wordt de betrokkene op de hoogte gesteld van de verwerking van zijn of haar persoonsgegevens en tevens op zijn rechten gewezen door toezending van de folder.

Bewaartermijn
In het register van verwerkingsactiviteiten staan per categorie van persoonsgegevens bewaartermijnen vermeld. Deze termijnen worden nu door medewerkers bewaakt en opgevolgd. Het streven is om systematisch de hand te houden aan deze termijnen en de signalering van verstreken bewaartermijnen in onze informatiesystemen op te nemen. In het kader van recht op vergetelheid is het belangrijk dat dit proces goed, vanuit archief, bewaakt wordt.

6.2 Privacy risico´s van te voren in kaart brengen
Voor (veranderingen in) processen, diensten, producten en informatiesystemen, waar persoonsgegevens worden gebruikt, is het van belang van te voren goed te bedenken welke privacyaspecten een rol (kunnen) spelen, welke effect het gebruik heeft op de privacy en welke oplossingen ervoor zorgen dat privacy problemen zich niet voordoen. De gemeente doet dit door:
- Business Impact Assessment (classificatie) uit te voeren
- Gegevensbeschermingseffectbeoordelingen (Privacy Impact Analyses (PIA) of Data Privacy Impact Assesment (DPIA) uit te voeren
- Bij het ontwerp rekening te houden met privacy aspecten en bij standaardinstellingen de privacy maximaal te waarborgen (Privacy by design of privacy by default).

Data classificatie (Business Impact Assesment)
Om te bepalen wat belangrijke processen zijn voor de organisatie, worden er classificaties uitgevoerd. Classificatie vindt plaats op proces, applicatie en/of data. Aan de hand van de classificaties kunnen mogelijke risico's in kaart worden gebracht en te treffen maatregelen worden geprioriteerd. De maatregelen die getroffen moeten worden om de gegevensbescherming te kunnen borgen, zijn niet voor elk proces en informatiesysteem hetzelfde.
Daarom is het nodig dat alle processen en informatiesystemen die gegevens verwerken een dataclassificatie ontvangen. Dataclassificatie heeft als doel om de continuïteit, integriteit en vertrouwelijkheid van het proces en het informatiesysteem te benoemen. Dit maakt inzichtelijk welke maatregelen genomen moeten worden om de gegevens die verwerkt worden te beschermen.
De CISO voorziet elk proces en informatiesysteem van dataclassificatie zoals deze is voorgeschreven door de Informatiebeveiligingsdienst.

Privacy Impact Analyse (PIA) & Data Privacy Impact Assesment (DPIA)
Voor een proces/product/dienst/systeem waarbij persoonsgegevens worden gebruikt en waarbij hoge privacy risico's spelen moet een PIA worden uitgevoerd. Een systematische beschrijving van het beoogde gebruik van persoonsgegevens, de doeleinden, de noodzaak en de proportionaliteit van het gebruik van persoonsgegevens, de risico's en (voorgenomen) maatregelen. Het doel is om de impact van het gebruik op de bescherming van persoonsgegevens in kaart te brengen.
Per PIA wordt advies aan de FG gevraagd.

Voor de verwerking van (gevoelige) persoonsgegevens wordt periodiek een gegevensbeschermings effectbeoordeling, ofwel Data Privacy Impact Assessment (DPIA) uitgevoerd. Dit is verplicht voor nieuwe

informatiesystemen, als een bestaande verwerking verandert of de risico's van een bestaande verwerking veranderen. Met de DPIA wordt het gebruik van het informatiesysteem getest op de effecten op de privacy van de betrokkenen. Voor het houden van een DPIA wordt overleg gepleegd met de Functionaris Gegevensbescherming.
Als wij, zonder dat een DPIA is gehouden, constateren dat persoonsgegevens in een systeem onvoldoende zijn beveiligd, bijvoorbeeld door een technische inregeling in de automatische verwerking van persoonsgegevens, dan doen wij ons best om het systeem zo spoedig mogelijk op dat punt te verbeteren en treffen wij zo nodig maatregelen om (verdere) ongewenste verwerkingen te voorkomen.
Om te weten of er een DPIA moet worden uitgevoerd worden er dataclassificaties uitgevoerd door de privacy officer. Hiermee worden mogelijke risico's in kaart gebracht.

Privacy by design & privacy by default
Privacy by design houdt in dat vanaf het ontwerpen van een nieuw of aangepast proces, product, dienst of informatiesysteem wordt nagedacht over:
° het rechtmatig, behoorlijk en transparant gebruiken van persoonsgegevens;
° de maatregelen die hiervoor nodig zijn.

Privacy by default betekent dat de standaard instellingen in systemen zo zijn ingesteld dat privacybescherming maximaal is geborgd.
Bij het toepassen van Privacy by design en – default wordt advies aan de FG gevraagd.

6.3 Maatregelen

Geheimhouding
Personen die toegang hebben tot persoonsgegevens zijn verplicht tot geheimhouding over die persoonsgegevens waarvan zij kennis kunnen nemen, tenzij de wet tot verstrekking verplicht of zijn taak daartoe noodzaakt. Medewerkers werkzaam voor de gemeente tekenen hiertoe een geheimhoudingsverklaring/integriteitsverklaring.
De gemeente vraagt medewerkers om een Verklaring Omtrent het Gedrag (VOG).

Bewustwording (awareness) en gedrag
Veilig verwerken van persoonsgegevens kan niet gegarandeerd worden zonder aandacht te geven aan het gedrag van de medewerkers en bestuursorganen. De mens is hierbij de zwakste schakel.
Wij werken aan de bewustwording van privacy gevoeligheid van persoonsgegevens door onder andere het geven van workshops. Daarin zijn de medewerkers over de vereiste basiskennis op grond van de actuele wetgeving geïnformeerd en zijn zij op een interactieve manier aan het denken gezet over het gedrag dat daarbij hoort. Deze workshop gaat over veilig werken in de breedste zin van het woord en wordt sinds 2017 gegeven en vormt een vast onderdeel van de Zeist Academie.
Verder zijn er algemene interne en toegankelijke richtlijnen en protocollen beschikbaar over het omgaan met persoonsgegevens op de werkplek en over datalekken.
Bij de introductie van nieuwe medewerkers wordt ook aandacht gevestigd op de veilige verwerking van persoonsgegevens. Privacy en Informatieveiligheid zijn beiden opgenomen in het inwerkprogramma.
Aanvullend hebben we AVG on tour, waarbij de juristen met soms ook de privacy officer de afdelingen langsgaan om te praten over de nieuwe privacywet en de gevolgen voor de werkprocessen.

Uitwisseling en delen van persoonsgegevens met derden
Als persoonsgegevens moeten worden uitgewisseld met (keten)partners, zoals zorginstellingen of politie, dan geldt daarvoor een privacy protocol. Als deze partijen (derden) voor en namens ons persoonsgegevens verwerken, worden er verwerkersovereenkomsten gesloten. Daarin zijn en worden afspraken opgenomen over de eisen die gelden voor de verwerking van persoonsgegevens. Dat zijn dezelfde eisen als waaraan wij zelf als gemeente moeten voldoen.

Wij blijven, als verwerkingsverantwoordelijke, verantwoordelijk voor de verwerking van de persoonsgegevens door een derde. Deze is dus verantwoording over de wijze van verwerking verschuldigd aan ons. Wij blijven ook verantwoordelijk voor de behandeling van verzoeken van betrokkenen aan die derde, ter uitvoering van zijn rechten.

Sinds medio 2018 beschikken wij over de technische voorziening om e-mails versleuteld te kunnen verzenden. Deze mogelijkheid wordt standaard aangeboden, wordt niet afgedwongen maar naar eigen inzicht van de medewerker gebruikt. Er is een sterk advies, zeker in bepaalde processen daar waar persoonsgegevens betreft, om wel gebruik te maken van veilig mailen.

Register van verwerkingen
Zeist heeft sinds mei 2017 een register van verwerkingen van persoonsgegevens. Dit register is op basis van reeds ontwikkelde registers (landelijk en collega gemeenten) opgebouwd door de privacy officer en wordt door hem ook onderhouden. In dit register staat een overzicht van alle processen

waarbij persoonsgegevens worden gebruikt en is daarmee een registratie van alle verwerkingsactiviteiten van persoonsgegevens die onder onze verantwoordelijkheid plaatsvinden.

Concreet staan daarin vermeld:
- de beschrijving van de verwerking (een activiteit, systeem of taak van de gemeente), bijvoorbeeld: salarisadministratie, postregistratiesysteem, jeugdhulp;
- de categorie van persoonsgegevens;
- de categorie van betrokkenen;
- de categorie van ontvangers van de persoonsgegevens;
- het doel en de grondslag van de verwerking;
- de bewaartermijn.

En geeft dus inzicht in de stromen van persoonsgegevens die gepaard gaan met gemeentelijke activiteiten en in de rechtmatigheid van deze verwerking. Dit register is openbaar. Inwoners hebben hierdoor inzicht in de wijze waarop hun persoonsgegevens worden gebruikt. Indien inwoners inzage willen, kan dit door een verzoek in te dienen bij de Functionaris Gegevensbescherming.

Verwerkersovereenkomst (VWO)
De gemeente is eindverantwoordelijke als zij doel en middelen vaststelt van het gebruik van persoonsgegevens. Ook als gebruik wordt gemaakt van leveranciers. De leverancier is dan een verwerker en het is wettelijk verplicht met hem een (verwerkers) overeenkomst af te sluiten. Hierin worden onder andere afspraken gemaakt over beveiliging, doelen van gebruik, toezicht, locatie van data, datalekken, geheimhouding. De gemeente gebruikt in beginsel het model verwerkersovereenkomst van de Informatiebeveiligingsdienst (IBD), deze is recentelijk als standaard door CVNG realisatie vastgesteld.

Technische maatregelen
Zonder technische maatregelen in de gebruikte informatiesystemen kan niet aan de waarborgen zoals hiervoor omschreven worden voldaan. Ons beleid met betrekking tot de fysieke beveiligingsmaatregelen van onze informatiesystemen staat in het Informatieveiligheidsbeleid. Op deze plaats halen wij enkele van die veiligheidsmaatregelen naar voren.

Wij hebben een informatieclassificatiesysteem waarmee de behoefte, de prioriteit en de mate van beveiliging van informatiesystemen kan worden bepaald. Aan de hand van de classificatie van informatiestromen kunnen per informatiesysteem en per niveau van vertrouwelijkheid maatregelen worden getroffen. Daarmee kan het juiste beveiligingsniveau van de informatiesystemen worden geborgd.

Autorisatie voor de toegang tot informatiesystemen wordt verleend op grond van de rol van de medewerker. Binnen het informatiesysteem krijgt de medewerker alleen toegang tot de functionaliteit en gegevens die nodig zijn voor de uitvoering van zijn of haar eigen rol of taken. Alle medewerkers hebben een individueel gebruikersprofiel zowel op netwerk als op applicatieniveau waardoor mutaties en zo mogelijk ook raadplegingen zijn terug te herleiden tot een individu.
Elk geautomatiseerde systeem dat persoonsgegevens verwerkt, moet logging bijhouden van de verwerkingen. In deze logging staat minimaal vermeld welke gebruiker, op welke moment, welke gegevens heeft verwerkt. Logging houdt in: chronologische registratie van gegevens over van belang zijnde gebeurtenissen, die zich gedurende een periode in een verwerking voordoen en het vastleggen in een log, bijvoorbeeld een systeem log of een security log, van feitelijk uitgevoerde bewerkingen en/of pogingen daartoe.

Er gelden richtlijnen voor de beveiliging van mobiele informatiesystemen zoals laptops, usb sticks, mobiele telefoons. Deze apparatuur is voor wat betreft de gemeentelijke informatie beveiligd. Deze richtlijnen worden regelmatig onderzocht op werkzaamheid en actualiteit.

Continue zijn we bezig om de digitale werkomgeving veilig te houden.
Voor meer informatie over ons Informatieveiligheidsbeleid verwijzen wij naar het Informatieveiligheidsbeleid op onze website [link] *https://www.zeist.nl/organisatie-bestuur/privacy/*

6.4 Toezicht en advies
Toezicht en advies
Om de bescherming van persoonsgegevens te waarborgen houdt de FG intern toezicht op de naleving van de privacyregelgeving. De FG beschikt daarbij over alle bevoegdheden die uit de wetgeving voortvloeien, zoals het doen van onderzoek, betreden van ruimtes, vragen van inlichtingen. De FG deelt zijn bevindingen met de verantwoordelijken en geeft zo nodig aanbevelingen en advies. De FG brengt

jaarlijks verslag uit over de naleving van de privacyregelgeving aan het college van burgemeester en wethouders. De gemeente toetst haar inzet jaarlijks normatief. Dit doet ze door gebruik te maken van het Privacy Control Framework (NOREA). Door middel van een Collegeverklaring wordt de Raad geïnformeerd.

Melding beveiligingsincidenten en datalekken (meldpunt datalekken)
Wij hebben een protocol en instructie voor medewerkers voor het geval er toch iets misgaat en er een beveiligingsincident is. Vanaf begin 2016 heeft Zeist een protocol en meldpunt datalekken. Medewerkers en inwoners kunnen beveiligingsincidenten melden bij het interne meldpunt datalekken. Bestuurlijk wordt benadrukt om dit positief te labelen om de drempel voor melden laag te houden). Het meldpunt onderzoekt of er sprake is van een datalek en bepaalt de strategie, al dan niet in overleg met management of bestuurder. Dat is het geval bij een inbreuk op de beveiliging waardoor de beveiliging van persoonsgegevens niet meer kan worden gegarandeerd. Voorbeelden daarvan zijn: een ontvreemd wachtwoord, verlies van datadragers of een hack van buitenaf. Afhankelijk van de ernst van de gevolgen voor de privacy van betrokkenen wordt het datalek gemeld bij de Autoriteit Persoonsgegevens en worden ook de betrokkenen zelf op de hoogte gebracht van het datalek en wat dit voor hen kan betekenen. Beveiligingsincidenten worden gelogd en in een register geplaatst.
Wij doen er uiteraard alles aan om de gevolgen van een lek te beperken en herhaling te voorkomen.

7. Organisatie (governance)

Met de inrichting van de organisatie rondom privacy wordt vastgelegd waar de verantwoordelijkheden liggen, wie welke taak heeft. Dit om uit te voeren beleid en taken te borgen en te beheren, zodat privacy gewaarborgd blijft.

7.1 Verantwoordelijkheden

Gemeenteraad
De gemeenteraad controleert of er voldoende wordt gedaan op het gebied van privacy bewustwording en of de AVG-maatregelen correct worden uitgevoerd. Zo kan de Gemeenteraad controleren wat de stand van zaken is van de risico's en maatregelen rondom gegevensbescherming. En of gegevens beschermende maatregelen aan de orde is (geweest) in de verschillende gemeentelijke kadernota's en begrotingsramingen.

College van Burgemeester en wethouders
De rechtspersoon/overheidsinstantie die het doel en de middelen voor het gebruik van persoonsgegevens vaststelt is verwerkingsverantwoordelijke" in de zin van de AVG.
De gemeente kent verschillende bestuursorganen die zelf voor bepaalde processen zelf de doelen en middelen vaststellen. Omdat burgemeester en wethouders in het algemeen binnen de gemeente het orgaan is die doel en middelen vaststellen zijn zij bestuurlijk eindverantwoordelijk voor de bescherming van persoonsgegevens binnen de gemeente.

Ook voor persoonsgegevens die door derden worden gebruikt is het college eindverantwoordelijk, als zij het doel en de middelen van het gebruik vaststellen. Het college stelt daarom het privacy beleid vast en mandateert de feitelijke verantwoordelijkheid aan de managers. Het college informeert de raad en legt verantwoording af aan de raad via de P&C cyclus.

Het management
De managers zijn feitelijk verantwoordelijk voor het juiste, zorgvuldige en veilige gebruik van persoonsgegevens, voor wat betreft de bij het team betrokken processen waarbij persoonsgegevens worden gebruikt.
De teammanager is eindverantwoordelijk voor:

- de melding aan de Privacy Officer van de bij zijn/haar programma betrokken processen waarbij persoonsgegevens worden gebruikt, deze komen uiteindelijk terecht in het register van verwerkingen en bij de Functionaris Gegevensbescherming (FG);
- afsluiten van verwerkersovereenkomsten als wordt ingekocht en het gebruik van persoonsgegevens onderdeel is van de geleverde dienstverlening;
- melding van beveiligingsincidenten aan de Chief Information Security Officer (CISO) en datalekken aan de Functionaris Gegevensbescherming (FG);
- sturen op privacy bewustzijn en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- het uitvoeren van een analyse op de (nieuwe en bestaande) verwerking om de beschermende maatregelen te bepalen.

Waar nodig wijzen ze privacy beheerders aan en fungeren ze als escalatiepunt met betrekking tot de naleving van de maatregelen voor de bescherming van persoonsgegevens

Medewerkers
De medewerkers van de organisatie zijn ieder verantwoordelijk voor hun eigen handelen. Ze worden geïnformeerd over procedures en werkwijzen en passen deze toe op de uitvoering van hun werkzaamheden.

7.2 Taken en rollen

Functionaris Gegevensbescherming (FG)
Het college heeft een functionaris gegevensbescherming in de zin van artikel 37 AVG benoemd. Het is van belang dat de FG-taken, zoals onafhankelijk toezicht, gescheiden zijn van de adviserende en uitvoerende taken van de CISO, PO en PJ.

De belangrijkste wettelijke taken van een FG (verplicht voor overheidsinstanties en -organen) zijn:
- Informeren en adviseren over de wettelijke verplichtingen bij het verwerken van persoons gegevens en toezien op naleving ervan;
- Toezien op een adequate beveiliging van gegevens en adviseren over betrouwbare ICT (privacy by design);
- Organiseren van een (verplichte) Privacy Impact Assessment (PIA) vóór het starten met nieuwe verwerkingen van persoonsgegevens, waarbij mogelijke risico's voor de privacy van betrokkenen worden geïnventariseerd;
- Als aanspreekpunt fungeren voor privacy vragen, zowel intern voor de organisatie zelf als extern voor de betrokkenen waarvan persoonsgegevens verwerkt worden;
- Samenwerken met de Autoriteit Persoonsgegevens (AP).

Voor het toezicht op de juiste verwerking van persoonsgegevens hebben wij samen met de gemeenten Bunnik, De Bilt, Utrechtse Heuvelrug en Wijk bij Duurstede de wettelijk verplichte Functionaris Gegevensbescherming (FG) aangesteld. Er zijn twee FG's die in de vijf gemeenten het toezicht uitoefenen en daarover rapporteren aan de Autoriteit Persoonsgegevens. De FG houdt toezicht en adviseert over de naleving van de privacywetgeving.

Privacy Officer (PO)
Voor de informatiebeveiliging zijn zogenaamde beveiligingsbeheerders aangesteld. Binnen de gemeenten fungeren de beveiligingsbeheerders tevens als vooruitgeschoven posten voor privacy. Ook anderen dan beveiligingsbeheerders kunnen zijn aangewezen als privacy officer (beheerder). Zij zijn de contactpersoon voor de FG en fungeren als aanspreekpunt voor de bescherming van persoonsgegevens De privacy officer is lid van het meldpunt datalekken, houdt het register van verwerkingen bij en voert de dataclassificaties uit.

Privacy jurist (PJ)
De privacy jurist heeft een rol bij privacy beleid, juridische beoordelingen van wijzigingen in regelgevende en/of zakelijke vereisten, privacyverklaring, gebruik en beperking, verzoeken op basis van de AVG (adviesrol), dus inzage, correctie, verwijdering, dataportabiliteit, verwerkersovereenkomsten en bijbehorende processen (en beschrijvingen).

Chief Information Security Officer (CISO)
Het kunnen borgen van de privacy kan niet gerealiseerd worden zonder adequate informatiebeveiliging. Het algemeen privacy beleid hangt samen met het Informatiebeveiligingsbeleid. Het Informatiebeveiligingsbeleid wordt vastgesteld door het college van burgemeester en wethouders en is gebaseerd op de richtlijnen van de BIG

Het informatiebeveiligingsbeleid wordt jaarlijks worden geëvalueerd. In dit Informatiebeveiligingsbeleid staan beveiligingseisen opgenomen die gelden voor informatiesystemen, gedragscodes en richtlijnen hoe de ambtelijke organisatie moet omgaan met (privacy)gevoelige informatie en de fysieke maatregelen die noodzakelijk zijn. De CISO houdt toezicht op de informatiebeveiliging en rapporteert hierover aan het management. Hij/zij bewaakt de voortgang van aanbevelingen uit het Informatiebeveiligingsplan en adviseert over het te voeren beleid. De CISO bevordert concern breed het beveiligingsbewustzijn door een PDCA aanpak op basis van risicosturing