Gemeente Zeist

GEMEENTEBLAD

Officiële uitgave van de gemeente Zeist

Nr. 533354
14 december
2023

Strategisch Privacy beleid Gemeente Zeist 2022-2026

1. Kernpunten

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 (persoons)gegevens omgaat.

In deze beleidsnotitie *"Strategisch Privacy beleid gemeente Zeist 2022-2026"*, geeft de gemeente Zeist de kaders aan voor de verwerking van persoonsgegevens die binnen de verantwoordelijkheid vallen van de gemeente. Het geeft op strategisch niveau duidelijkheid en daarmee sturing aan de inrichting van privacy en Gegevensbescherming en de keuzes die daarbij gemaakt worden. Dit is van belang om te waarborgen dat de verwerking van persoonsgegevens op een rechtmatige wijze plaatsvindt conform de geldende wet- en regelgeving. Dit vervangt het *Privacybeleid Gemeente Zeist uit 2019*.

1.1 Leeswijzer

Hoofdstuk 1 benoemt de kernpunten van het privacybeleid, waaronder visie, doel en uitgangspunten van het beleid. Hoofdstuk 2 beschrijft aan welke voorwaarden processen en systemen moeten voldoen en hoe dit beleid wordt toegepast. In hoofdstuk 3 is beschreven wat de verantwoordelijkheid voor privacy inhoudt. Dit biedt kaders voor het handelen van de gemeente. Hoofdstuk 4 besteedt aandacht aan het toezicht op de naleving van privacyregels en hoe controle op de uitvoering plaatsvindt. In hoofdstuk 5 gaat in op de positie van de betrokkenen van wie persoonsgegevens worden verwerkt.

1.2 Doel

Het doel van dit privacybeleid is om te waarborgen dat de gemeente Zeist persoonsgegevens verwerkt op een rechtmatige en behoorlijke wijze en dit kan aantonen. De gemeente biedt de juiste bescherming aan onze burgers en medewerkers over wie persoonsgegevens worden verwerkt. De organisatie en processen worden gebruiksvriendelijk ingericht. Hiermee wordt de privacywetgeving nageleefd en invulling gegeven aan actuele privacy principes voortvloeiend uit geldende wetgeving en jurisprudentie.

1.3 Visie

De visie van gemeente Zeist op de bescherming van persoonsgegevens hangt nauw samen met de rol van de gemeente in een moderne Informatiesamenleving, zoals verwoord in het *'ambitiedocument: Een goed leven in Zeist – ook digitaal '*.[1]

Uitgangspunten zijn onze kernwaarden: vertrouwen, nabijheid en kracht. Dit vraagt om een omgang met privacy op maat waarbij telkens opnieuw afwegingen worden gemaakt en waarbij gezocht wordt naar het juiste evenwicht door gebruik te maken van het moreel kompas (het goede doen).
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 gemeente Zeist zich te allen tijde een betrouwbare partner toont.

Inwoners verwachten van ons dezelfde dienstverlening als van de beste bedrijven. We zien de overgang van diensteneconomie naar de netwerk- en informatiesamenleving. De digitalisering is in volle gang en verandert de samenleving in rap tempo. Daarmee verandert ook de verhouding gemeente, inwoners en bedrijven. Ontwikkelingen als big data, internet of things, robotisering en smart villages zullen een steeds grotere impact hebben op onze samenleving. Maar ook het werk van (de medewerkers van) onze gemeente verandert drastisch.

Deze ontwikkelingen vragen een meer empathische en minder afstandelijke lokale overheid. Een gemeente die minder gericht is op procedures en regels, en beter inspeelt op de persoonlijke omstandigheden van (groepen) inwoners. Een overheid die dichtbij is en een bijdrage levert tussen de vele horizontale netwerken in de samenleving. Maar ook een overheid die steeds nadrukkelijker inspeelt op de

1) Het ambitiedocument 'Een goed leven in Zeist – ook digitaal' beschrijft hoe we ons (digitale) bewustzijn en onze (digitale) weerbaarheid kunnen verhogen en beschrijft de dilemma's die we hierbij tegenkomen. Dit ambitiedocument wordt in 2023 in een werksessie met het college besproken en na vaststelling door het college wordt er een themabijeenkomst georganiseerd met de Raad.

technologische ontwikkelingen. Een belangrijke opgave voor gemeenten is het werken aan een samenleving waar iedereen naar vermogen mee kan doen. Een samenleving waar mensen tot hun recht komen. Waarbij het niet meer volstaat dat we ons alleen richten op **wat** we doen (openbare orde & veiligheid, wonen & omgeving, maatschappelijke ondersteuning, belastingheffing, enzovoorts), maar ook **hoe** we dat (gedigitaliseerd) organiseren.

Bescherming van persoonsgegevens en respect voor de privacy is voor ons een sleutelstrategie en een kwestie van behoorlijk bestuur. Zonder persoonsgegevens of bij gebrekkige informatievoorzieningen functioneren wij niet of niet goed. Mensen ervaren ons dan op een slechte manier en lopen in meer of mindere mate risico's, terwijl wij ook bestuurlijke risico's lopen. Maatschappelijk verantwoorde, kwalitatief goede en daarnaast ook veilige gegevensverwerking is rand voorwaardelijk. De Algemene Verordening Gegevensbescherming reikt ons hiervoor de handvatten aan. Met dit privacy beleid maken wij de vertaalslag van wet naar praktijk.

- Gemeente Zeist waarborgt bescherming van persoonsgegevens en respect voor privacy in alle geledingen van haar bedrijfsvoering, zowel intern als in de samenwerking met haar ketenpartners.
- Gemeente Zeist is transparant over haar gegevensverwerking en betrekt personen via haar AVG-dienstverlening, zodat zij fouten tot een minimum beperkt en sprake is van een individueel medebeheer over persoonsgegevens. Gemeente Zeist gaat de dialoog aan met haar doelgroepen en werkt aan een volwassen gegevensbeschermingscultuur. Zij dient steeds met vertrouwen verantwoording te kunnen afleggen over beleid en maatregelen op het gebied van Gegevensbescherming en AVG naleving.
- Met de ambitie van gemeente Zeist om de bedoeling van de Algemene Verordening Gegevensbescherming na te leven, wordt handen en voeten gegeven aan de invulling van het goede leven in Zeist en excellente dienstverlening.
- Betrokkenen, zoals onder meer inwoners en medewerkers, moeten erop kunnen vertrouwen dat gemeente Zeist persoonsgegevens rechtmatig, zorgvuldig en veilig verwerkt. Gemeente Zeist is transparant over gegevensverwerkingen en de manier waarop zij persoonsgegevens beschermt.
- Bij dilemma's met betrekking tot de verwerking van persoonsgegevens gaat gemeente Zeist de dialoog met betrokkenen aan en zoekt zij, waar mogelijk, gezamenlijk naar oplossingen.
- Privacy gaat iedereen wat aan. Dit gaat niet alleen over elkaar maar vooral met elkaar (verbinden). Dit door zorgvuldig, bewust om te gaan met gegevensverwerking en privacy. Het wordt vertaald naar het borgen in (primaire) processen, vastleggen in de verwerkingsregistratie en transparantie naar de burgers (vertrouwen).
- Gemeente Zeist gaat op een veilige manier met persoonsgegevens om en respecteert de persoonlijke levenssfeer van betrokkenen/inwoners en medewerkers. Gemeente Zeist houdt zich hierbij aan de wettelijke uitgangspunten, en stelt de bedoeling boven de systemen (vertrekken vanuit de ander). Het borgen en uitvoeren van de wettelijke taken wordt gezien als een uitdaging en niet als belemmering. Gemeente Zeist kijkt naar oplossingen en mogelijkheden.

1.3 Uitgangspunten

Op grond van artikel 24 AVG moet privacybeleid passend zijn voor de verwerkingen die onder verantwoordelijkheid van de gemeente worden uitgevoerd en rekening houden met risico's voor de rechten en vrijheden van betrokkenen. Dit beleid sluit aan bij het normenkader voor de overheid op het gebied van informatiebeveiliging: de Baseline Informatiebeveiliging Overheid (BIO). Waarbij vooral wordt aangesloten bij de uitgangspunten voor de operationele borging van privacy binnen de organisatie. Dit is een continu proces. Risicomanagement is een belangrijk onderdeel hierin.

Hieruit vloeien de volgende uitgangspunten voort:

- Zorg voor privacy is een verantwoordelijkheid van bestuur en (lijn)management. Zij sturen op Gegevensbescherming volgens deze kernpunten van privacy management:
  - De formele eindverantwoordelijkheid berust bij de afzonderlijke bestuursorganen van de gemeente. Het college van B&W stelt de uitgangspunten van het privacybeleid vast,
  - Een proceseigenaar voert, als onderdeel van zijn verantwoordelijkheden, regie en houdt toezicht op zijn proces(sen) op basis van dit privacybeleid;
  - Binnen een proces worden gegevens alleen verwerkt voor het realiseren van het procesdoel;
  - Binnen een proces worden geen onrechtmatig verkregen gegevens verwerkt;
  - Incidenten worden door het Meldpunt datalekken volgens de procedure afgewikkeld.

- Er is voorzien in een team van professionals (2de lijns) dat het college en de proceseigenaren ondersteunt in de privacy beleidsvoering.

- Het borgen van privacy in de uitvoering van gemeentelijke processen vindt risico gestuurd plaats. De verantwoordelijken in de organisatie maken afwegingen ter naleving van privacyregels en op basis van een risico-inschatting.
- Het college handhaaft het privacybeleid en informeert de raad over de privacy beleidsvoering.
- Er wordt voorzien in communicatie over het beleid en faciliteiten voor bewustwording en training, zodat iedere medewerker conform het privacybeleid kan handelen.
- De gemeente Zeist beschikt over procedures voor privacy incidentmanagement, zodat adequaat gehandeld kan worden in geval van datalekken.
- Jaarlijks wordt dit beleid getoetst en na 3 jaar een evaluatie op doeltreffendheid en doelmatigheid.
- De gemeente Zeist heeft een Privacy officer in dienst voor de borging van privacy in de organisatie.
- Gemeente Zeist heeft een Functionaris voor Gegevensbescherming aangesteld die in onafhankelijkheid toeziet op naleving van de AVG, gerelateerde wetgeving en nakoming van afspraken volgens dit privacybeleid.

1.4 Scope

Het strategisch beleidskader is:

- van toepassing op de gehele bedrijfsvoering van gemeente Zeist, voor zover hierbij gewerkt wordt met persoonsgegevens;
- is de kapstok waaraan aanvullende regelingen zijn opgehangen zoals regelingen voor het uitoefenen van rechten;
- omvat zowel bedrijfsprocessen als de onderliggende voorzieningen voor informatieverwerking en gegevensopslag. Papieren of digitale informatieverwerking maakt geen verschil;
- is van toepassing op processen die de gemeente uitbesteedt, inkoopt of organiseert;
- is van toepassing op gegevensuitwisseling met derden zoals Belastingdienst, de Raad voor de Kinderbescherming, politie en zorgaanbieders, met dien verstande dat na legitieme en zorgvuldige gegevensverstrekking door de gemeente, de verantwoordelijkheid voor de bescherming van persoonsgegevens vanaf het moment van ontvangst bij die derde berust;
- omvat de gehele ‘data life cycle’: van het genereren of verzamelen van gegevens, het dagelijkse gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging ervan;
- is van toepassing op de verwerking van statistische en/of geanonimiseerde gegevens, voor zover niet kan worden uitgesloten dat personen kunnen worden geïdentificeerd of geprofileerd;
- is eveneens van toepassing op Informatieveiligheidsvraagstukken, voor zover deze betrekking hebben op het verwerken van persoonsgegevens.

1.5 Raakvlakken en overlap met andere beleidsthema’s

Het Privacybeleid Gemeente Zeist heeft raakvlakken met diverse andere beleidsthema’s of vertoont hiermee overlap.

- *Integriteit:* Privacy beleidsvoering is wettelijk gekoppeld aan de beginselen van behoorlijk bestuur en is daarmee ondersteunend aan het gemeentelijk integriteitsbeleid, zoals beschreven in de gedragscode Integriteit van Gemeente Zeist.
- *Kwaliteit:* Privacy beleid richt zich in belangrijke mate op het waarborgen van een kwalitatief goede administratieve organisatie. Deze is rand voorwaardelijk voor klantgerichte en klantvriendelijke gemeentelijke taakuitoefening en goed werkgeverschap (‘de mens centraal’).
- *Continuïteit- en risicomanagement:* Privacy beleid schept waarborgen op het gebied van continuïteit en risicomanagement, omdat privacybeleid afbreuk- en aansprakelijkheidsrisico’s tegengaat en voorkomt dat werkprocessen spaak lopen omdat de bijbehorende gegevensverwerkingen een schending van het recht op privacy inhouden (onrechtmatige overheidsdaad).
- *Informatieveiligheid:* Privacybeleid ondersteunt het informatieveiligheidsbeleid door het tegengaan van privacy incidenten die de beschikbaarheid, integriteit en vertrouwelijkheid aantasten van de gemeentelijke informatievoorzieningen en opgeslagen persoonsgegevens. Ten aanzien van informatieveiligheid geldt het Informatieveiligheidsbeleid van gemeente Zeist.
- *Personeel en organisatie:* Het sturen op gekwalificeerd personeel, cultuur en een gekwalificeerde organisatie wordt uitgevoerd vanuit het HRM beleid.
- *Communicatie:* Het sturen op doelgroepgerichte communicatie wordt gedaan vanuit het communicatie beleid Gemeente Zeist.
- *Inkoop:* Het inkoopbeleid regelt de samenwerking derden. Hierbij worden eisen gesteld aan de waarborgen die de betreffende derde partij kan bieden.
- *Archivering:* Het zorgen dat er sprake is van een matchende en duurzame informatievoorziening. Waarbij de basis op orde is.

2. Privacy beleid gemeente Zeist

De gemeente Zeist is zich bewust van de maatschappelijke verantwoordelijkheid die gepaard gaat met de verwerking van persoonsgegevens. Daarom voert gemeente Zeist proactief privacybeleid op basis van dit beleidskader en wordt naleving van wet- en regelgeving bewaakt. De gemeente Zeist faciliteert de uitoefening van rechten van personen.

2.1 Begrippen

Voor de begripsvorming een korte toelichting van enkele AVG-begrippen:

Persoonsgegevens: informatie over een geïdentificeerde of identificeerbare persoon (de betrokkene). Het gaat hierbij om ieder gegeven dat te herleiden is tot een bepaald natuurlijk persoon. Zoals naam, adres, woonplaats etc.

Bijzondere persoonsgegevens zijn privacygevoeliger, bijvoorbeeld gegevens over gezondheid, strafrecht (waaronder gegevens uit registers van politie en justitie), religie of etniciteit. Deze zogenaamde bijzondere gegevens mag de gemeente daarom alleen verwerken in de gevallen dat dit wettelijk is toegestaan.

'Verwerking' omvat alle handelingen met persoonsgegevens, waaronder verzamelen, opslaan, verstrekken en vernietigen van de gegevens. Verzamelen vindt vaak plaats bij een aanvraag of melding en soms ook doordat de gemeente navraag doet. De verwerking vindt plaats door de verwerker:

Verwerkingsverantwoordelijke: Is een persoon of instantie die het doel van en middelen voor de verwerking van persoonsgegevens vaststelt. De bestuursorganen van de gemeente zijn verwerkingsverantwoordelijken voor de verwerkingen die door of namens de gemeente worden uitgevoerd.

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

2.2 Eisen aan gegevensverwerking

Proceseigenaren verwerken persoonsgegevens voor zover dit noodzakelijk is voor het realiseren van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde publieke taken, de nakoming van wettelijke of contractuele verplichtingen, vrijwaring van vitale belangen voor de betrokkene(n), totstandkoming of uitvoering van een overeenkomst waarbij een burger partij is of de behartiging van een gerechtvaardigd belang van gemeente Zeist of een derde aan wie gegevens worden verstrekt, tenzij het recht op de bescherming van de persoonlijke levenssfeer prevaleert en voor zover het gerechtvaardigd belang geen grondslag voor de uitoefening van een publieke taak vormt.

Verwerkingen van persoonsgegevens vinden plaats in overeenstemming met AVG beginselen. Het gaat dan om eisen benoemd in artikel 5 AVG:

a) **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 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.

b) **Transparantie**
Voor de betrokken burger moet duidelijk zijn wat er met de persoonsgegevens gebeurt. Het is van belang dat de burger (proactief) geïnformeerd wordt over het doel van de verwerking van diens gegevens, welke gegevens nodig zijn en met wie gegevens noodzakelijkerwijze gedeeld gaan worden. De informatieplicht richting de burger is in de procesinrichting van gemeente Zeist en haar partners voorzien. En worden betrokkenen geïnformeerd via gemeentelijke informatiekanalen. 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 zorgt voor het waarborgen van deze rechten.

c) **Doelbinding**
De gemeente Zeist verzamelt persoonsgegevens alleen voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel en verstrekt deze gegevens alleen voor zover dat binnen het doel is toegestaan. Afwijkend gebruik voor ándere doelen is slechts mogelijk na afweging van de wettelijke criteria. Deze afweging gebeurt in de vorm van een 'verenigbaarheidstoets' conform artikel 6 lid 4 AVG.

d) **Noodzakelijk en proportioneel**
De gemeente Zeist verwerkt alleen die gegevens die strikt noodzakelijk om het doel waarvoor ze nodig zijn te bereiken. De gegevensverwerking moet toereikend, ter zake dienend en niet bovenmatig zijn. Gemeente Zeist hanteert daarbij de regel 'need to know' in plaats van 'nice to know'. Bij de beoordeling van een gegevensverwerking spelen de beginselen van proportionaliteit en subsidiariteit (voor de betrokkene minst ingrijpende middel inzetten om bepaald doel te bereiken).

e) **Zorgvuldigheid, behoorlijkheid, juistheid**
Persoonsgegevens moeten altijd juist, volledig en actueel zijn. In de diverse processen vinden controles plaats om te verifiëren dat de juiste persoonsgegevens gebruikt worden.

f) **Opslagbeperking en bewaartermijnen**
De gemeente Zeist bewaart gegevens volgens de wettelijk geldende termijnen of anders altijd zo kort mogelijk en 'vernietigt' deze daarna. In diverse wetten zijn bewaartermijnen opgenomen. Voor persoonsgegevens in archiefwaardige bescheiden geldt een bewaartermijn die is vastgesteld in de 'Selectielijst voor gemeenten en intergemeentelijke organen', vastgesteld op grond van de Archiefwet.

g) **Integriteit en vertrouwelijkheid**
De gemeente Zeist neemt passende technische of organisatorische maatregelen zodat persoonsgegevens integer en vertrouwelijk worden verwerkt. Daarbij horen ook maatregelen ter beveiliging van de persoonsgegevens. Bij het nemen van maatregelen ter beveiliging van gegevens zijn de BIO en het informatieveiligheidsbeleid van de gemeente Zeist richtinggevend.

2.3 Risico gedreven aanpak

De privacy beleidsvoering van gemeente Zeist is erop gericht om aantoonbaar te voorzien in passende organisatorische en technische maatregelen voor doeltreffende bescherming van persoonsgegevens en de bescherming van rechten van personen. Dit vergt een risico gedreven aanpak.

Wat 'passend' is, hangt af van de concrete risico's die de verwerking van persoonsgegevens voor mens en organisatie met zich meebrengt. Deze worden vastgesteld op basis van objectieve beoordelingen – aan de hand van Data Protection Impact Assessments (DPIA's). Hiermee wordt inzichtelijk of een gegevensverwerking is te classificeren als laag, midden of hoog risico en of het te mitigeren van deze risico's een inspanning vereist die laag, midden of hoog is. Door het uitvoeren van een risico classificatie krijg je dit inzicht.

Bij nieuw in te stellen processen wordt privacy vanaf het begin van het ontwerpproces meegenomen, door na te denken over de benodigde technische en organisatorische maatregelen en die in te bouwen in processen en systemen (denk hierbij aan 'privacy by design' en 'privacy by default').

Aan nieuwe verwerkingen en risicovolle processen liggen data protection impact assessments (DPIA's) ten grondslag. DPIA's zijn instrumenteel voor het inzichtelijk krijgen van het proces, de omgang met persoonsgegevens daarin met bijbehorende risico's en om passende beheersmaatregelen te bepalen. De mate waarin en manier waarop bedrijfsprocessen en gegevensverwerking aandacht nodig hebben, hangt samen met de uitkomsten van de DPIA. De rapporten worden opgesteld conform artikel 35 lid 7 AVG.

Met behulp van de aanbevelingen in het DPIA-rapport wordt voorzien in passende organisatorische en technische privacybeschermende maatregelen. Voor processen met een laag privacy risico volstaan algemene oplossingen. Zolang een proces als laag risico gekwalificeerd is, is daarvoor in mindere mate aandacht nodig.

De risico gestuurde aanpak voorkomt dat in strijd met privacynormen en privacy principes wordt gehandeld, bijvoorbeeld bij:

- Onrechtmatige gegevensverwerking, zoals wanneer er een verbod of beperking geldt voor gebruik, opslag of uitwisseling van persoonsgegevens;

- Disproportionele gegevensverwerking, zoals (a) ontoereikende of bovenmatige gegevensverwerking of (b) gegevensverwerking waarbij het organisatiebelang onevenredig klein is in verhouding tot de impact van de verwerking op personen;
- Irrelevante gegevensverwerking, zoals gegevensverwerking voor niet ter zake dienende of verouderde doeleinden;
- Onnauwkeurige gegevensverwerking, zoals wanneer de gebruikte, opgeslagen of uitgewisselde gegevens geen juiste weergave van de werkelijkheid bieden;
- Onveilige gegevensverwerking, zoals wanneer gegevens toegankelijk zijn of dreigen te worden voor onbevoegden waardoor misbruik mogelijk is;
- Niet-inachtneming van bijzondere wettelijke voorschriften, zoals niet-nakoming van meldplichten, wettelijke termijnen, toestemmingsverplichtingen;
- Onbewaakte gegevensverwerking, zoals wanneer niet gecontroleerd wordt of privacy waarborgende maatregelen geëffectueerd zijn of bijstelling behoeven.

2.4 Gegevensuitwisseling bij samenwerking

Het beleid van de gemeente Zeist richt zich in belangrijke mate op het samen met andere overheidsorganisaties en sociale partners aanpakken van sociale, maatschappelijke en veiligheidsvraagstukken. In de samenwerkingsverbanden die daardoor ontstaan komen ook casussen van individuele burgers aan de orde en zullen indien noodzakelijk hun persoonsgegevens worden gedeeld. Dit kan ook aan de orde zijn wanneer er binnen de organisatie samengewerkt wordt bij specifieke thema's, opgaven en programma's.

Bij de uitvoering moet rekening gehouden worden met de wettelijke privacy voorschriften die van toepassing zijn op de gemeente zelf en op haar partners waarmee samengewerkt wordt. Deze privacyregels kan en wil de gemeente Zeist niet negeren, maar stelt haar wel voor dilemma's in de uitvoering van bepaalde werkzaamheden, zoals:

- bij gegevensuitwisseling die nodig is in het kader van integrale dienstverlening die de gemeente nastreeft, bijvoorbeeld in het sociaal domein;
- bij de handhaving van vergunningen, ruimtelijke voorschriften en de openbare orde en veiligheid.

Als uitgangspunt van handelen bij dit soort dilemma's hanteert de gemeente de volgende werkwijze:

- De gemeente zorgt ervoor dat het verwerken van gegevens, waaronder de uitwisseling van gegevens bij externe of interne samenwerking, binnen de kaders van de verschillende wetten kan plaatsvinden.
- Mochten de wetten niet in de uitwisseling van gegevens voorzien, dan valt de gemeente Zeist terug op de mogelijkheid van artikel 6 lid 4 AVG: het uitvoeren van een verenigbaarheidstoets. Bekeken wordt dan of gebruik van de gegevens mogelijk is voor ándere doelen dan de oorspronkelijke doelen waarvoor de gegevens verzameld zijn in de uitvoering van de taak. Gegevensuitwisseling met derden kan dan mogelijk worden.
- Wanneer het gaat om verwerkingen die een hoog risico voor betrokkenen inhouden, wordt een data protection impact assessment (DPIA) uitgevoerd. Een DPIA maakt inzichtelijk welke maatregelen er nodig zijn om op een rechtmatige en zorgvuldige manier met persoonsgegevens om te gaan, inclusief de uitwisseling met derden.

Deze uitgangspunten legt de gemeente Zeist vast in zowel privacy convenanten als het gaat om het delen van gegevens met externen als in privacyreglementen voor het delen van gegevens binnen de eigen organisatie. De afspraken in deze documenten integreert de gemeente in haar werkprocessen.

2.5 Inachtneming bijzondere wettelijke voorschriften

Op basis van het Privacy beleid Gemeente Zeist, geeft de gemeente uitvoering aan de Algemene Verordening Gegevensbescherming (AVG) en de Wet Politie Gegevens (WPG). Voor zover van toepassing, houden proceseigenaren tevens rekening met bijzondere wettelijke voorschriften – met name privacyrelevante bepalingen in de Wet basisregistratie personen, Telecommunicatiewet, Participatiewet, Jeugdwet en Wet maatschappelijke ondersteuning enzovoort.

3. Taken, rollen en verantwoordelijkheden

Het beleidskader is van toepassing op het college van B&W, de burgemeester en de gemeenteraad en op de ambtelijke organisatie van de gemeente Zeist en is het uitgangspunt van handelen. De uitvoering van het privacybeleid is onderdeel van de bedrijfsvoering van de ambtelijke organisatie en het handelen van de griffie en volgt de verantwoordelijkheidslijnen van de mandaatbesluiten.
Zoals is te lezen in onderstaand schema zijn er verschillende rollen en verantwoordlijkheden te onderscheiden.

Tabel verantwoordelijken (RASCI) en 3-lijnen model (ofwel Three Lines of Defence (3LoD)).[2]

RASCI	3 / LoD	Rolverdeling
R – Responsible (operationeel verantwoordelijk)	1ste lijn	• Proceseigenaren / Lijnmanagement • Medewerkers • Uitvoeringsorganisaties ('verwerkers')
A Accountable (bestuurlijk eindverantwoordelijk)	1ste lijn	• Het college (verwerkingsverantwoordelijke)
S Supportive (ondersteunend)	2de lijn	• Team Veilig werken, ICT, informatieveiligheid, Inkoop, JZ, risk en kwaliteit management
C Consulted /Toezicht lemand die geraadpleegd wordt	3de lijn	• FG (i.s.m. audit)
I *Informed iemand die geïnformeerd wordt*	*4e lijn*	• *Inwoners, De raad; Accountant;* • *Autoriteit Persoonsgegevens (AP)*

3.1 Verantwoordelijkheid voor verwerking

De AVG kent het begrip 'verwerkingsverantwoordelijke'. De verwerkingsverantwoordelijke is verantwoordelijk voor de verwerking van persoonsgegevens in overeenstemming met wetgeving, regelingen en beleid op het gebied van privacy. En stelt doel en middelen vast voor de verwerkingen van persoonsgegevens.
De bestuurlijke en strategische verantwoordelijkheid berust bij het college van B&W en de gemeenteraad. Zij dragen zorg voor passend gemeentelijk privacybeleid. Binnen het college is een portefeuillehouder aangewezen. Het college legt over de uitvoering van het privacybeleid verantwoording af aan de gemeenteraad. Privacy heeft zelfstandige aandacht in de planning- en control cyclus.

3.2 Bestuurlijke verantwoordelijkheid

Het college van gemeente Zeist is verantwoordelijk voor de naleving van privacywetgeving en voert proactief beleid op basis van afweging van belangen en risico's bij de verwerking van persoonsgegevens, zodat dit evenwichtig plaatsvindt. Dat wil zeggen: behoorlijk, zorgvuldig en in overeenstemming met de wet en vanuit de kernwaarden van onze organisatie: Vertrouwen, Nabijheid en Kracht.
Het college is verantwoordelijk voor het voorzien in passende privacy waarborgen bij de uitvoering van gemeentelijke taken. En legt verantwoording af over privacy beleidsvoering aan de raad en betracht beleidstransparantie met behulp van publieksvoorlichting.
Documentatie van beleid en maatregelen vindt plaats, zodat op ieder moment, zowel vooraf als achteraf, maatschappelijk en juridisch uitleg kan worden gegeven over de aanpak.

3.3 Verantwoording gemeentelijke organisatie

De verantwoordelijkheid van het college van B&W wordt praktisch vertaald naar de (uitvoerende) ambtelijke organisatie. Waarbij de lijnmanagers een belangrijke rol hebben als eigenaar van het proces. Het college verwacht van proceseigenaren een rechtmatige en zorgvuldige verwerking van persoonsgegevens. Proceseigenaren kunnen hiervoor rekenen op support vanuit team Veilig werken binnen afdeling IV en de FG. Proceseigenaren zorgen in samenwerking met team Veilig werken voor passende organisatorische en technische oplossingen om de rechtmatigheid, proportionaliteit, juistheid en veiligheid van gegevensverwerking te waarborgen ('privacy waarborgen') en documenteren in samenwerking met de 2de lijn de genomen maatregelen.

Het college is transparant over de bedrijfsvoering, gegevensverwerking en privacy beleidsvoering en faciliteert de uitoefening van rechten door personen over wie de gemeente gegevens verwerkt. Proceseigenaren verlenen hieraan hun medewerking. Het college en proceseigenaren dragen het belang uit van privacy beleidsvoering en geven zelf het goede voorbeeld. Zij maken privacy bespreekbaar. Bij dilemma's gaan zij de dialoog aan met doelgroepen over wie informatie wordt verwerkt.

Proceseigenaren zijn ervoor verantwoordelijk dat de gemeentelijke taakuitoefening waarvoor zij verantwoordelijk zijn, binnen de grenzen van dit beleidskader plaatsvindt. Zoals gezegd blijft het college

2) ***RASCI is de afkorting van Responsible (verantwoordelijke), Accountable (eindverantwoordelijk), Supportive (ondersteunend), Consulted (iemand die geraadpleegd moet worden) en Informed (iemand die geïnformeerd moet worden).***

eindverantwoordelijk voor de privacy bestendigheid van gemeentelijke processen als de ‘verwerkingsverantwoordelijke’ in de zin van de AVG. Maar het zijn de lijnmanagers die als 'Proceseigenaren' op uitvoeringsniveau verantwoordelijk zijn voor de privacy bestendige bedrijfsvoering en gegevensuitwisseling met derden.

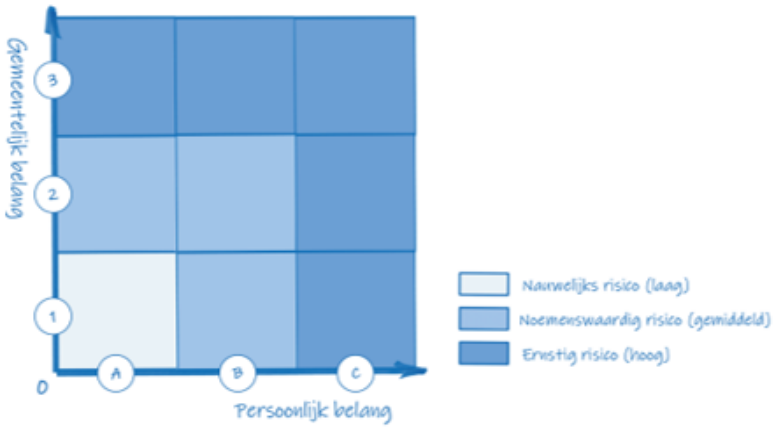
Privacy raakt aan informatieveiligheid, hier vindt dan ook nauwe afstemming mee plaats. Voor informatiebeveiliging is een CISO (Chief Information Security Officer) aangesteld. Tevens is er de Functionaris Gegevensbescherming (FG) aangesteld als toezichthouder.

3.4 Privacy officer

Voor de operationele ondersteuning en aansturing op het gebied van privacy is er een privacy officer. De Privacy Officer geeft samen met Team Veilig werken ondersteuning aan proceseigenaren over een privacy bestendige uitvoering van de processen.
De privacy officer houdt het Register van verwerkingen bij, voert Quick scans uit, ondersteunt bij het uitvoeren van DPIA’s en is lid van het Meldpunt datalekken.

a) **Het Gegevensverwerkingsregister (artikel 30 register)**
De privacyofficer onderhoudt en beheert het gegevensverwerkingsregister” (‘artikel 30-register’). Dit register valt onder de eindverantwoordelijkheid van het college en wordt getoetst door de FG. De proceseigenaren dienen, om het register volledig en actueel te laten zijn, hun verwerkingen en veranderingen in de verwerkingen, aan te leveren.
Het Gegevensverwerkingsregister dient een overzicht te bevatten van alle processen waarbij persoonsgegevens worden gebruikt en is daarmee een registratie van alle verwerkingsactiviteiten van persoonsgegevens die onder de verantwoordelijkheid van de gemeente Zeist plaatsvinden. Het register geeft dus inzicht in de stromen van persoonsgegevens die gepaard gaan met gemeentelijke activiteiten en in de rechtmatigheid van deze verwerking. Het register is openbaar en wordt beschikbaar gesteld via de website, zodat inwoners hierdoor inzicht hebben in de wijze waarop hun persoonsgegevens worden gebruikt.

b) **Data Protection Impact Assesment (DPIA)**
DPIA staat voor “data protection impact assessment“ en is een beoordelingsrapport waarin een gegevensverwerking wordt geanalyseerd op noodzaak en risico’s vanuit privacy optiek, resulterend in een overzicht van passende beheersmaatregelen (waarborgen).



DPIA’s zijn instrumenteel voor het kunnen bepalen van passende beheersmaatregelen. De mate waarin en de manier waarop bedrijfsprocessen en gegevensverwerking aandacht nodig hebben, hangen samen met de uitkomsten van de DPIA, zoals verwoord in het DPIA-rapport.
DPIA-rapporten worden opgesteld conform artikel 35 lid 7 AVG.

Voor een eenduidig begrip hanteert gemeente Zeist een DPIA-scoringssysteem. Hoe hoger de score, hoe robuuster de beheersmaatregelen (privacy waarborgen). Proceseigenaren volgen het advies van Team Veilig werken bij de vaststelling van hun DPIA-score. DPIA-scores worden bepaald aan de hand van bovenstaande matrix. Proceseigenaren documenteren hoe zij op een praktische manier in passende organisatorische en technische privacybeschermende maatregelen voorzien. Voor A1-processen (nauwelijks risico, laag, met een lage score op zowel persoonlijk als gemeentelijk belang) volstaan algemene oplossingen. Veranderingen in de bedrijfsvoering noodzaken tot aanpassing van procesplannen, waarvoor een nieuwe of geactualiseerde DPIA nodig is.

c) **Verwerkingsovereenkomst (VWO)**
De gemeente is (en blijft) eindverantwoordelijke als zij doel en middelen vaststelt van het gebruik van persoonsgegevens. Ook als zij de verwerking niet zelf uitvoert (denk aan leverancier of ge-

meenschappelijke regeling of ketenpartner). Deze derde partij is dan een verwerker en het is wettelijk verplicht om dan een Verwerkers overeenkomst af te sluiten met deze partij.
De verwerkersovereenkomst is de overeenkomst tussen verantwoordelijke en verwerker, waarin wordt vastgelegd hoe de verwerker met de persoonsgegevens moet omgaan en afspraken gemaakt over het gebruik en de beveiliging van gegevens, doelen van gebruik, toezicht, locatie van data, datalekken en geheimhouding. De gemeente maakt gebruikt van de standaard VNG model verwerkersovereenkomst. Het VWO is onderdeel van een overeenkomst.

d) **Meldpunt datalekken**
In het geval van een datalek voldoet de gemeente aan de meldplicht, conform artikelen 33 en 34 AVG. Er is een Meldpunt datalekken waar een ieder terecht kan bij een datalek of vermoeden van een datalek. Er is een procedure ingesteld voor het melden van datalekken. Indien nodig wordt melding gedaan bij de AP en worden betrokkenen geïnformeerd. Alle datalekken worden bijgehouden in een register.

4. Toezicht

Landelijk toezicht wordt uitgevoerd door de Autoriteit Persoonsgegevens (AP). Het gemeentelijk toezicht wordt uitgevoerd door de functionaris voor Gegevensbescherming (FG), de wettelijk verplichte (interne) toezichthouder. Daarnaast zijn er interne controles op toepassing van de privacynormen.

4.1 Controle op werking en naleving

Het beleid, procedures en maatregelen worden steekproefsgewijs en periodiek getoetst op opzet, bestaan en werking in de praktijk. Een periodieke toets op het onderdeel privacy vindt plaats aan de hand van het kwaliteitssysteem. Verantwoordelijken in de organisatie dienen ook zelf periodiek te (laten) controleren in hoeverre de feitelijke situatie in overeenstemming is met toepassing van het privacybeleid. De toetsing aan de hand van het kwaliteitssysteem helpt hen hierbij. Daarnaast zijn vragen, klachten, incidentmanagement, verenigbaarheidstoetsen en DPIA's (zie 2.3) steekproefsgewijze toetsing van naleving van het privacybeleid.

4.2 Verdere verwerking, archiefbeleid, gegevensvernietiging

Het college voorziet samen met Proceseigenaren in, met passende waarborgen omklede, verdere verwerking van gegevens voor verenigbare doelen zoals het genereren van managementinformatie. Ook wordt voorzien in, met passende waarborgen omklede, oplossingen voor archivering en adequate oplossingen voor gegevensvernietiging.

De overgedragen archieven berustend bij het gemeentearchief, vallen vanaf het moment van overbrenging onder de Archiefwet en zijn daarmee in beginsel openbaar. De AVG blijft echter van toepassing. Er wordt conform AVG gehandeld in zowel het beheer als in de dienstverlening.
Het beleidsstuk dat hieraan ten grondslag ligt is 'Beleidsnotitie AVG en het gemeentearchief' (zaaknummer: 100893).

4.3. Privacy audit

Vragen, klachten en het incidentmanagement zijn in wezen steekproefsgewijze toetsing van de privacy beleidsvoering. Om niet voor verrassingen te worden geplaatst, is het belangrijk om regelmatig te toetsen in hoeverre beleidsvoering en de feitelijke situatie met elkaar overeenstemmen aan de hand van privacy audits op de gehanteerde ijkpunten.
Zie het onderstaande schema voor de benodigde zwaarte en frequentie van privacy audits.

	Type audit	Frequentie	Betrokkenheid FG	Afschrift FG
A1	Quick scan	5 jaarlijks	-	-
A2	Zelfevaluatie	4 jaarlijks	Vrijwillig	Vrijwillig
A3	Audit	3 jaarlijks	Ja	Ja
B1	Zelfevaluatie	5 jaarlijks	Vrijwillig	Ja
B2	Zelfevaluatie	4 jaarlijks	Ja	Ja
B3	Audit	3 jaarlijks	Ja	Ja
C1	Audit	4 jaarlijks	Ja	Ja
C2	Audit	3 jaarlijks	Ja	Ja
C3	Audit	2 jaarlijks	Ja	Ja

- Bij een gegevensverwerking met kwalificatie nauwelijks risico (laag), volstaat een quickscan. De quickscan is een beknopte toets onder de verantwoordelijkheid van de Proceseigenaar
- Bij een gegevensverwerking met kwalificatie noemenswaardig risico (gemiddeld), volstaat een zelfevaluatie. Een zelfevaluatie is een uitgebreidere toets onder verantwoordelijkheid van de Proceseigenaar.
- Bij een gegevensverwerking met kwalificatie ernstig risico (hoog), volstaat een audit. Audits worden door de Proceseigenaar georganiseerd in samenwerking met Team Veilig werken

4.2 Functionaris Gegevensbescherming

De functionaris Gegevensbescherming (FG) is de (interne) toezichthouder van gemeente Zeist. En voert zijn rol en taken uit conform artikelen 37 tot en met 39 AVG. De FG is formeel aangesteld en vanuit de organisatie de contactfunctionaris voor de landelijk toezichthouder; de Autoriteit Persoonsgegevens.

Conform artikel 37 lid 5 AVG is de FG aangewezen op grond van: (a) zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de privacy management-praktijk; (b) zijn vermogen om de onderstaande taken te vervullen en (c) zijn onafhankelijkheid, met name de afwezigheid van een belangenconflict.

Vanwege zijn expertise van wetgeving en de praktijk, geldt een advies van de FG als zwaarwegend en de geëigende wijze voor naleving van privacywetgeving door de gemeente Zeist. De FG doet jaarlijks verslag van zijn werkzaamheden aan het college van B&W. Het college besluit over bijstelling van het gemeentelijk privacybeleid met inachtneming van de aanbevelingen van de FG.

5. Privacy services

Een fundamenteel uitgangspunt, dat opgenomen is in de AVG, is dat verwerking van persoonsgegevens ‘ten dienste van de mens’ staat. Mede hierom moeten betrokkenen controle over hun eigen persoonsgegevens hebben.

5.1 Rechten van betrokkenen

Betrokkenen van wie de gemeente gegevens verwerkt mogen ervan uitgaan dat dit in overeenstemming met privacyregels gebeurt. Tevens zijn in de AVG specifieke privacyrechten voor personen opgenomen. Betrokkenen hebben er recht op:

- Dat gemeente handelt conform het onderhavige privacy beleid;
- dat gemeente Zeist handelt conform het onderhavige privacy beleid;
- dat zij informatie verschaft over doelen van informatieverwerking en privacy beleidsvoering;
- dat zij inzage in hun eigen gegevens hebben;
- dat zij – in geval van fouten – hun gegevens kunnen (laten) verbeteren of verwijderen;
- om tegen het gebruik van hun gegevens verzet aan te tekenen, wat gemeente Zeist verplicht tot het maken van een afweging;
- dat zij gemeente Zeist bij niet-naleving van het gemeentelijk privacy beleid (of de wet) hierop mogen aanspreken.

In het Protocol Persoonsgegevens gemeente Zeist wordt nader beschreven welke rechten betrokkenen toekomen en welke procedures hiervoor gelden binnen gemeente Zeist (Persoonsgegevens en privacy (zeist.nl)

5.2 Vragen en/of klachten

Inwoners hebben altijd de mogelijkheid om vragen te stellen over de verwerkingen van persoonsgegevens. Dit verloopt via de coördinator bij het KCC van de gemeente. Beantwoording van de vragen vindt in samenwerking met de proceseigenaar plaats. Er kan advies gevraagd worden van het team Veilig werken of de FG.

Met klachten over de verwerking van persoonsgegevens door de gemeente kan men ook altijd terecht bij de gemeente. Betrokkenen kunnen contact opnemen met de FG over aangelegenheden die verband houden met de verwerking van hun persoonsgegevens en met de uitoefening van hun rechten voortvloeiende uit AVG.
Tevens hebben personen altijd het recht een klacht in te dienen bij de landelijke toezichthouder, de AP.

Bijlage 1. Addendum privacybeleid WPG

Inleiding
Vanaf 25 mei 2018 geldt de Algemene Verordening Gegevensbescherming (AVG). De gemeente heeft in haar privacy beleid en informatieveiligheidsbeleid vastgelegd hoe zij omgaat met bescherming van persoonsgegevens.
De verwerking van persoonsgegevens door buitengewoon opsporingsambtenaren (boa's) valt niet alleen onder de AVG maar ook onder de Wet politiegegevens (Wpg). Daarnaast is een aantal andere regelingen van toepassing op de verwerking van politiegegevens. Zoals het Besluit politiegegevens (Bpg), het Besluit politiegegevens buitengewoon opsporingsambtenaren en de Regeling periodieke audit politiegegevens. Deze wetten en regelgevingen kennen op enkele gebieden wat onderlinge verschillen.

Zo kent de Wpg bijvoorbeeld specifieke bewaartermijnen voor de opslag van politiegegevens, terwijl de AVG geen concrete bewaartermijnen voorschrijft[3]. Ook stelt de Wpg andere eisen bij het delen van politiegegevens tussen verschillende partijen, is er een verplichting tot logging en zijn er in de Wpg aanvullende beperkingen en uitzonderingen op de in de AVG geldende privacyrechten van betrokkenen. Andere verplichtingen zijn vergelijkbaar maar kennen verschillen in de concrete uitwerking, zoals de verplichting voor de verwerkingsverantwoordelijke om passende technische en organisatorische maatregelen te treffen ter bescherming en beveiliging van de gegevens. In het kader van de Wpg is bijvoorbeeld ook eens per 4 jaar een externe audit verplicht en moeten elk jaar interne audits worden gehouden.

Doelstellingen van het privacy beleid
Het privacy beleid van de gemeente beschrijft hoe we verantwoordelijk en binnen wettelijke kaders met persoonsgegevens omgaan. Voor de reikwijdte van dit addendum bestaat het wettelijk kader voor bescherming van persoonsgegevens uit de Wpg en genoemde regelingen. De gemeente wil met dit addendum op het privacy beleid onder andere bereiken dat de boa's:
- Zich ten volle bewust zijn van de noodzaak om zorgvuldig en op rechtmatige wijze om te gaan met politiegegevens;
- De rechten van betrokkenen respecteren en werken volgens de vastgestelde procedures;
- Het vertrouwen van betrokkenen in de overheid niet beschamen.
- Gedrag vertonen dat past bij goed werknemerschap.
- De kans op financiële en imagoschade minimaliseren.

Wpg kader
Het normenkader van de Wpg is grotendeels gelijkluidend aan dat van de AVG. Op hoofdlijnen geldt aanvullend nog het volgende:
- De boa's van de gemeente kunnen naast hun opsporingstaken ook bestuursrechtelijke toezichts- en handhavingstaken hebben. Zij krijgen dan bij het verwerken van persoonsgegevens te maken zowel met de AVG te maken als met de Wpg;
- In de verwerking van gegevens moet duidelijk zijn welke gegevens er worden verwerkt onder de AVG en welke onder de Wpg. De Wpg stelt andere eisen aan de verwerking van persoonsgegevens dan de AVG. Zo geldt onder andere de plicht tot delen met ieder andere opsporingsambtenaar die deze gegevens nodig heeft voor zijn werk.

De hierna genoemde verplichtingen uit de Wpg zijn veelal geborgd binnen onze applicaties:
- Er moet een scheiding worden aangebracht tussen gegevens die op feiten zijn gebaseerd en feiten die op een persoonlijk oordeel zijn gebaseerd;
- Er moet onderscheid worden gemaakt tussen betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden;
- Documentatie is vereist van de doelen van onderzoeken, verstrekking of doorgifte, afwijzing van verzoeken om inzage, inbreuk op de beveiliging, doorgifte buiten de EU met datum en tijd, ontvanger, redenen en doorgegeven gegevens en melding van gemeenschappelijke verwerkingen aan de Autoriteit Persoonsgegevens (AP).
- Er vindt logging plaats in geautomatiseerde systemen van de invoer van gegevens in systemen en op termijn ook van het verzamelen, wijzigen, raadplegen, verstrekken (o.a. in de vorm van doorgifte), combineren of vernietigen van politiegegevens.
- Er worden specifieke eisen gesteld aan de informatiebeveiliging uit het Bpg.

Er geldt met ingang van 2021 een verplichting tot het uitvoeren van een externe privacy audits. De rapportage die hieruit voortvloeit moet worden verstrekt aan de AP. Als er tekortkomingen zijn geconstateerd dient er een verbeterplan te worden opgesteld waarop binnen het jaar hercontrole plaatsvindt.

3) *Het onderliggende privacy beleid van de gemeente Zeist gaat uit van de AVG. Dit is de reden dat gekozen is om dit addendum Privacy WPG met de richtlijnen en verplichtingen toe te voegen aan het Privacy beleid.*

De hercontrole geldt alleen voor die onderdelen van de wet waar de tekortkomingen geconstateerd worden. De resultaten van de hercontrole worden vastgelegd in een rapportage en eveneens verstrekt aan de AP, uiterlijk 1 jaar na het uitvoeren van de externe audit.

Register van verwerkingen
Net als de AVG verplicht de Wpg tot het bijhouden van een register van verwerkingen. Wel zijn er enkele verschillen die hierna met een (*) zijn aangeduid. Het register van verwerkingen in het kader van de Wpg moet het volgende bevatten:

- De naam en de contactgegevens van de verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de functionaris voor Gegevensbescherming;
- De doelen van de verwerking;
- De categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties;
- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- In voorkomend geval: het gebruik van profilering. (*)
- In voorkomend geval: de categorieën van doorgiften van politiegegevens aan een derde land of een internationale organisatie.
- Een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de politiegegevens bedoeld zijn. (*)
- Zo mogelijk: de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd.
- Zo mogelijk: een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging.
- De toekenning van de autorisaties. (*)

Informatieveiligheidsbeleid
Het informatiebeveiligingsbeleid is een richtinggevend en kaderstellend beleidsdocument. De gemeente vult het aan met beleid voor informatiebeveiliging op tactisch en operationeel niveau met specifieke (beleids-) documenten. Het informatiebeveiligingsbeleid geldt voor alle activiteiten van de gemeente. Ook voor de activiteiten die vallen onder de Wpg geldt dat passende technische en organisatorische maatregelen moeten zijn genomen en geïmplementeerd, op basis van een risicoanalyse waaruit het risiconiveau blijkt met betrekking tot ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging. Deze maatregelen moeten bovendien periodiek worden geëvalueerd en zo nodig geactualiseerd.

FG en bevoegd functionaris
Net als de AVG verplicht artikel 36 van de Wpg tot het aanstellen van de FG. De FG wordt door de verwerkingsverantwoordelijke tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van politiegegevens. De FG stelt jaarlijks een verslag op van zijn bevindingen en stelt het ter beschikking aan de verwerkingsverantwoordelijke.

De bevoegd functionaris is verantwoordelijk voor het uitvoeren van de taak bevoegd functionaris. Dit is de 'hoeder' van de gegevens die onder artikel 9 Wpg worden verwerkt. Deze functionaris is beschreven in artikel 2:10, eerste lid, van het Besluit politiegegevens (Bpg). Het moet een persoon zijn met voldoende kennis en vaardigheden over dit type gegevens. Deze functionaris beslist bijvoorbeeld wie er toegang mag hebben tot deze gegevens en of ze verstrekt kunnen worden aan een samenwerkingspartner. Iedere artikel 9-verwerking dient een bevoegd functionaris (BF) te hebben.
De bevoegd functionaris heeft onder andere de volgende taken:

- het doel van de artikel 9-verwerking omschrijven en vastleggen;
- het autoriseren van personen voor de betreffende verwerking;
- bepalen of gegevens voor andere doeleinden mogen worden gebruikt;
- zorgen dat voor alle gegevens de herkomst en wijze van verkrijgen wordt vastgelegd;
- bewaken dat gegevensrechtmatig worden verkregen en verwerkt

Rechten van betrokkenen
De rechten van betrokkenen onder de AVG staan uitgebreid beschreven in het privacy beleid van de gemeente. Op hoofdlijnen zijn deze rechten op grond van de Wpg gelijkluidend.

Het bewaren van politiegegevens
Politiegegevens worden niet langer bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. Politiegegevens dienen na verwijdering nog maximaal vijf jaar worden bewaard. Daarna, of binnen deze periode van vijf jaar (afhankelijk van welke bewaartermijn geldt) dient definitieve vernietiging plaats te vinden. Indien van cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens. Er wordt dan aan de bewaareisen als genoemd in de Archiefwet voldaan.

Alle politiegegevens worden gelabeld in artikel 8, 9 en 13 informatie. Voor elk label is de bewaartermijn conform de wettelijke bepaling geconfigureerd, zodat geborgd wordt dat deze politiegegevens niet langer worden bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt.
De overgedragen archieven berustend bij het gemeentearchief, vallen vanaf het moment van overbrenging onder de Archiefwet en zijn daarmee in beginsel openbaar. De AVG blijft echter van toepassing. Er wordt conform AVG gehandeld in zowel het beheer als in de dienstverlening. Het beleidsstuk dat hieraan ten grondslag ligt is 'Beleidsnotitie AVG en het gemeentearchief' (nr. 100893).

Het ter beschikking stellen en verstrekken van politiegegevens
De Wpg maakt een onderscheid tussen het ter beschikking stellen van politiegegevens en het verstrekken ervan. Het ter beschikking stellen van politiegegevens houdt in dat deze in principe worden gedeeld met eenieder die de gegevens nodig heeft voor de uitoefening van zijn taak. Bij dit 'need to know'-principe dient altijd een noodzakelijkheids-, proportionaliteits- en subsidiariteitsafweging te worden gemaakt. Het ter beschikking stellen voltrekt zich dus binnen het Wpg-domein.
Bij het verstrekken van politiegegevens gaat het om het delen van gegevens buiten het Wpg-domein. In dat geval moet zijn geborgd dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wpg en het Bpg zijn genoemd. Geborgd moet ook zijn dat wanneer gegevens verstrekt worden, er wordt voldaan aan de documentatieplicht en dat de verstrekking alleen plaatsvindt in overeenstemming met het bevoegd gezag indien dit vereist is in de wet. Het gaat dan bijvoorbeeld om verstrekkingen aan de burgemeester, een toezichthouder, een advocaat of een functionaris in het kader van de Wet bibob.

Het melden van datalekken
De datalek procedure onder de AVG is beschreven in het privacy beleid van de gemeente. Op hoofdlijnen zijn deze rechten op grond van de Wpg gelijkluidend. Specifiek voor de Wpg geldt nog het volgende: Op deze mededelingsplicht zijn enkele uitzonderingen van toepassing, onder andere als de mededeling achterwege moet blijven ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures en ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

Bewustwording
Het zorgvuldig omgaan met persoonsgegevens is enerzijds een kwestie van het organiseren van een goede informatieveiligheid en het zorgvuldig inrichten van werkprocessen, anderzijds is het een zaak van bewustwording bij de boa's. Het bewustzijn wordt voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.
Elke nieuwe medewerker dient een Wpg training te doorlopen. Boa's die al in dienst zijn en deze training nog niet hebben doorlopen, doorlopen deze training alsnog. Daarnaast is er in ieder geval jaarlijks aanvullend aandacht voor bewustwording rondom de omgang met politiegegevens. Dit kan bijvoorbeeld in de vorm van een aanvullende training, een bijeenkomst over een specifiek Wpg-onderwerp of in de vorm van een toets.

Open communicatie
Betrokkenen moeten erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden verwerkt. De gemeente creëert dat vertrouwen door inzichtelijk te maken, door middel van verschillende communicatiekanalen, op welke wijze zij persoonsgegevens verwerkt en beheert (zie o.a. de privacyverklaring die op de website is te vinden).