



Beleidsregels verwerking persoonsgegevens gemeente Nieuwegein 2026

Burgemeester en wethouders;

gelet op artikel 24, lid 2, van de Algemene verordening gegevensbescherming;

besluit:

vast te stellen

Beleidsregels verwerking persoonsgegevens gemeente Nieuwegein 2026

Bestuurlijke samenvatting

Volgens de AVG is het college van burgemeester en wethouders (soms raad of burgemeester) verwerkingsverantwoordelijk en is zij gehouden aan de verordening te voldoen. Deze bestuurlijke verantwoordelijkheid zal voor de dagelijkse sturing worden belegd bij de portefeuillehouder, die verantwoordelijk is voor digitaal verantwoorde en veilige informatie.

In de praktijk is privacy een issue dat op de werkvloer speelt. Uitgangspunt in dit beleidsplan is om de verantwoordelijkheid zo dicht mogelijk bij de uitvoering van de gemeentelijke processen te organiseren door het mandateren van taken en bevoegdheden aan de teammanagers. De concernadviseurs (de CISO, de concernjurist en Privacy Officer, de strategisch informatieadviseur, zie verderop voor specifieke taakhoud) bieden ondersteuning bij het inrichten van de kaders, zijn adviseurs voor technische en organisatorische kwesties, hebben een coördinerende rol in de bedrijfsvoeringscyclus en verwerken datalekken. Deze adviseurs werken risicogestuurd. De afdelingen zijn verantwoordelijk voor het inrichten van de interne processen, het opstellen van de juiste documenten (protocollen, verwerkingsovereenkomsten, etc.) en de archivering van persoonsgegevens.

Het college is verantwoordelijk voor het vaststellen van het privacy beleid. De directie is verantwoordelijk voor de uitvoering van het beleid. De betrokkenheid van directie bij de vormgeving van het privacy beleid bestaat uit het beoordelen van jaarplannen (uit te werken in de werkinstructies) die per afdeling wordt gemaakt en het accorderen van de inzet van middelen en het resultaat in het voorafgaande jaar. Deze verantwoording staat niet op zichzelf, maar wordt meegenomen in de reguliere P&C-cyclus van de gemeente.

De gemeente wil optimaal gebruik maken van de ruimte die de AVG biedt om persoonsgegevens te verwerken. Welke ruimte er precies is, ligt nog niet in beton gegoten.

Het uitgangspunt van de AVG is dat bij het ingrijpen in de persoonlijke levenssfeer er altijd een afweging wordt gemaakt tussen het algemene belang en of het gerechtvaardigde belang van de gemeente en dat van de betrokkene(n). Deze afweging zal worden gemaakt binnen de beleidsruimte van de AVG.

Ellie Liebrechts
secretaris

Marijke van Beukering-Huijbregts
Burgemeester

1. Inleiding

De gemeente werkt met (persoons)gegevens van burgers, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente voor het goed kunnen uitvoeren van de gemeentelijke wettelijke taken. Denk hierbij onder andere aan taken in het sociaal domein, het openbare orde en veiligheidsdomein of voor burgerzaken. Om deze taken goed te kunnen uitvoeren is het noodzakelijk dat de gemeente persoonsgegevens verwerkt. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Nieuwegein is zich hiervan bewust en wil daarom het eerdere vastgestelde beleid uit 2019 actualiseren.

Een belangrijk aandachtspunt in de AVG is het in lijn brengen van gemeentelijke taken waarbij persoonsgegevens worden verwerkt, het doel van de verwerking, de juridische grondslag voor de verwerking en de wijze waarop met een minimum aan persoonsgegevens het doel van de verwerking kan worden bereikt. Voor zo ver er risico's bij het verwerken van persoonsgegevens kunnen zijn is het uitgangspunt dat wij maatregelen nemen om de risico's zo veel mogelijk te beperken of te voorkomen. Als de risico's door de procesverantwoordelijken worden aanvaard motiveren de procesverantwoordelijken dit in een afgewogen onderbouwing en stemmen zij dit met het bestuur af.

Terugblik

De AVG is op 25 mei 2018 in werking is getreden. Het huidige beleid over privacy is op 11 december 2019 vastgesteld door het college, mede gebaseerd op de resultaten van een onderzoek naar de stand van zaken van het privacy management/ privacy kader. De aanbevelingen uit dit onderzoek zijn een belangrijke leidraad geweest voor het vormgeven van dat privacy beleid. Dit beleid kan getypeerd worden als een strategisch theoretisch kader op hoofdlijnen waarbij op onderdelen vanuit een theoretisch perspectief wordt beschreven hoe de gemeente invulling gaat geven aan dit beleid.

Doorontwikkeling

Het bestuur, management en medewerkers hebben ieder vanuit hun eigen rol de nodige ervaring opgedaan in de uitvoering van wettelijke taken waarbij de verwerking van de persoonsgegevens nodig is met inachtneming van de AVG en andere specifieke wetgeving over het verwerken van persoonsgegevens. Gaandeweg is er een beleidslijn ontwikkeld bij het veilig verwerken van persoonsgegevens en daarbij is een eenduidige manier ontwikkeld waarop de verantwoording over gevoerde privacybeleid plaatsvindt. Deze verantwoording zal verder vorm en inhoud moeten krijgen, in ieder op een zodanige wijze dat het past binnen de cultuur van de verschillende teams en afdelingen.

De maatschappelijke ontwikkelingen rondom privacybewust en digitaal veilig werken staan niet stil. De gemeente werkt steeds met verschillende data, die vaak ook persoonsgegevens bevatten. Hoe kan bijvoorbeeld kunstmatige intelligentie (Artificial Intelligence, AI) op een betrouwbare manier gebruikt worden door de gemeente. En wat zijn Europese wettelijke kaders daarvoor?

Het privacy beleid uitvoeren betekent in het dagelijks werk van medewerkers en leidinggevenden dat met in achtneming van de wettelijke kaders logisch nadenken en respectvol omgaan met de persoonsgegevens van de inwoners op een toegankelijke manier wordt verantwoord waarom persoonsgegevens worden of zijn verwerkt.

De onderdelen van het huidig privacy beleid die nog actueel zijn, zijn verwerkt in dit beleid.

2. Visie

De gemeenteraad heeft in het Manifest Digitaal Nieuwegein een belangrijk kader bepaald voor de manier waarop de gemeente de digitale samenleving samen met de stad vorm en inhoud wil geven. Daarom is het manifest een pijler van dit beleid. Het manifest bevat in feite het hoger doel waarom en hoe de gemeente omgaat met persoonsgegevens in een samenleving die steeds digitaler wordt.

De code voor goed openbaar bestuur, specifiek ten aanzien van veilig omgaan met persoonsgegevens (governance) en het uitwerken daarvan, is dat in een heldere structuur in de gemeentelijke organisatie blijkt wie verantwoordelijk is voor wat. Het gaat om regels die bepalen wanneer wij persoonsgegevens mogen gebruiken, hoe we persoonsgegevens mogen gebruiken en wat we moeten doen om aan te tonen dat we zorgvuldig omgaan met persoonsgegevens. Deze aspecten vatten we samen onder de noemer 'privacy management'.

Het borgen en het verbeteren van de privacybewustwording en de verdere professionalisering van de privacyfunctie in de organisatie zijn belangrijke speerpunten van het privacy management. Privacybewust en digitaal veilig werken is noodzakelijk voor het betrouwbaar functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Daarbij is het actueel houden van kennis over privacy en informatieveiligheid, verantwoord en bewust gedrag van medewerkers essentieel voor privacy binnen de gemeente. Iedereen werkzaam binnen de gemeente is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. De gemeente verlangt van al haar medewerkers en alle personen die werkzaam zijn voor de gemeente dat de voorschriften van dit privacybeleid worden opgevolgd en actief worden uitgedragen.

3. Doel

Met dit privacybeleid geeft de gemeente aan op welke wijze verantwoord omgegaan wordt met persoonsgegevens en hoe de persoonlijke levenssfeer van de personen waarvan de gemeente persoons-



gegevens verwerkt (of laat verwerken) wordt gewaarborgd. Daarnaast beoogt dit privacybeleid taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af te bakenen.

De verdere uitwerking van dit beleid is - waar relevant - vastgelegd in de operationele documenten binnen de gemeente, zoals handreikingen, protocollen, concrete werkprocedures of werkafspraken voor algemene onderwerpen zoals datalekken, maar ook domeinspecifieke onderwerpen als gegevensdeling voor de uitvoering van de Jeugdwet of de Wet maatschappelijke ondersteuning 2015.

4. Reikwijdte

De gemeente verzamelt en gebruikt persoonsgegevens van inwoners, leveranciers en medewerkers en andere natuurlijke personen (hierna te noemen: betrokkenen).

Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens de gemeente.

Het college van burgemeester en wethouders verleent mandaat en machtiging aan de algemeen directeur en de directeur bedrijfsvoering om de uitvoering van deze beleidsregels in een privacy protocol vast te stellen. Voor wat betreft onderwerpen die over openbare orde en veiligheid gaan mandateert en machtigt de burgemeester de algemeen directeur en de directeur bedrijfsvoering om de uitvoering van deze beleidsregels in een protocol vast te stellen.

Nadere uitwerking gegevensverwerking in het sociaal domein

De gemeente voert de volgende wetten uit waarbij het verwerken van persoonsgegevens in het sociaal domein aan de orde is om de toegang tot hulp en ondersteuning voor haar inwoners te realiseren:

- Wet maatschappelijke ondersteuning 2015 (Wmo 2015);
- Jeugdwet;
- onderdelen van de Participatiewet;
- Wet inburgering;
- Wet verplichte geestelijke gezondheidszorg;
- en andere wetgeving in het sociale domein die de gemeente dient uit te voeren.

Het uitgangspunt is dat inwoners met zorg- en ondersteuningsvragen optimaal geholpen worden, waarbij altijd (hulp)vraaggericht gewerkt wordt en de behoefte van de inwoner centraal staat. Er wordt ingezet op (het versterken van) de zelfredzaamheid en op preventie, zodat zwaardere problematiek zoveel mogelijk voorkomen wordt.

De gemeente heeft informatie nodig om te bepalen welke hulp een inwoner nodig. Daarbij is het nodig dat de inwoner gegevens verstrekt die betrekking hebben op de leefomstandigheden van de inwoner, diens familie of sociaal netwerk. In de praktijk is het gebruikelijk om een aanvraag over de verschillende leefdomeinen te doen. Dit staat op gespannen voet met het beginsel van dataminimalisatie uit de AVG. Daarom is het nodig dat binnen de kaders van de AVG, de Uitvoeringswet AVG, en de Wmo 2015 aparte beleidsregels worden geformuleerd voor de verwerking van persoonsgegevens bij het beoordelen van hulpvragen. De beleidsregels hebben betrekking op de volgende onderwerpen:

- a. De wijze waarop betrokkenen worden geïnformeerd over welke persoonsgegevens de gemeente verwerkt bij het beoordelen van hulpvragen voor jeugdhulp en maatschappelijke ondersteuning;
- b. Het behandelen van verzoeken van betrokkenen om hun persoonsgegevens in te zien, te corrigeren, te laten verwijderen of over te dragen;
- c. Het verwerken van persoonsgegevens van inwoners door derden.

5. Privacy en informatieveiligheid

Naast dit privacybeleid is het Strategisch informatiebeveiligings- en privacybeleid vastgesteld. Hierin zijn maatregelen opgenomen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens, zoals toegangsbeheer, versleuteling, logging, monitoring en leveranciersbeveiliging. Het gemeentelijke privacybeleid kan daarom niet los worden gezien van het gemeentelijke informatiebeveiligingsbeleid. Dit privacybeleid is de nadere uitwerking van het strategisch informatiebeveiligings- en privacybeleid.



6. Principes voor de verwerking van persoonsgegevens

De AVG is gebaseerd op een aantal principes voor de verwerking van persoonsgegevens. De gemeente onderschrijft deze principes en stelt zich ten doel persoonsgegevens te verwerken in overeenstemming met deze principes.

Rechtmatige grondslag

Persoonsgegevens worden door de gemeente slechts in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze verwerkt. Dit betekent onder meer dat verwerkingen slechts plaatsvinden als hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking bij een gemeente voort uit een wet (wettelijke verplichting) of een publiekrechtelijke taak.

Welbepaalde doeleinden

De gemeente verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen. Dit betekent dat de gemeente alleen die persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken (ter zake dienend). De gemeente ziet af van de verwerking als het doel op een andere – minder ingrijpende – wijze kan worden bereikt, bijvoorbeeld door minder of geen persoonsgegevens te verwerken en indien hetzelfde doel op een andere – minder ingrijpende – wijze kan worden bereikt, bijvoorbeeld door het anonimiseren of aggregeren van gegevens. Bij anonimiseren kan bijvoorbeeld gedacht worden aan gebruik van nummers in plaats van namen. Een voorbeeld van het aggregeren van persoonsgegevens is om inwoners in een bepaalde stad te groeperen op hun gedeelde kenmerken, interesses en voorkeuren te bepalen. Daarbij geldt telkens dat er wettelijke grondslag voor het verwerken van persoonsgegevens moet zijn.

Verdere verwerking

Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor deze persoonsgegevens in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, of dat hiervoor extra waarborgen zijn getroffen. De gemeente voert, voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

Minimale gegevensverwerking

Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiest de gemeente bij voorkeur voor die mogelijkheid. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een voor de betrokkene minder inbreuk makende wijze kan worden verwezenlijkt dan kiest de gemeente bij voorkeur voor die mogelijkheid.

Juiste en actuele gegevens

De gemeente zorgt ervoor dat alleen persoonsgegevens worden verwerkt die accuraat, toereikend, ter zake dienend en niet bovenmatig zijn gelet op het doel waarvoor zij verzameld zijn of vervolgens worden verwerkt. De gemeente neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

Gegevens worden op tijd vernietigd

De gemeente stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en de selectielijsten. Gemeenten hebben op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard.

Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt de gemeente de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. De gemeente bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

Integriteit en vertrouwelijkheid

De gemeente neemt passende technische en organisatorische maatregelen om de persoonsgegevens, met name bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. De gemeente handelt hierbij in overeenstemming met het informatiebeveiligingsbeleid <link>. Het informatiebeveiligingsbeleid verplicht de gemeente om informatie te beveiligen tegen

ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking.

Privacy by Default en Privacy by Design

De gemeente houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van persoonsgegevens. Dit uitgangspunt wordt *Privacy by design* (PbD) genoemd. De gemeente draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de gemeente *Privacy by Default* als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

Toegang tot gegevens

Uitsluitend geautoriseerde gebruikers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend. Deze bevoegdheden worden verleend op grond van het binnen de gemeente geldend beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Het beheer van bevoegdheden wordt periodiek gecontroleerd. De gemeente hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens, om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

Inbreuk in verband met persoonsgegevens

Bij toegang tot, verlies of wijziging van persoonsgegevens bij de gemeente, zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet, afhankelijk van het risico, worden gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens) en soms bij de getroffen betrokkenen. De gemeente registreert datalekken, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan. Datalekken worden behandeld volgens het privacyprotocol. In dit protocol is vastgelegd wie een datalek moet melden, welke termijn geldt en welke informatie minimaal nodig is en wie beoordeelt of een melding aan de Autoriteit Persoonsgegevens of aan betrokkene verplicht is.

Samenwerking

De gemeente schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregulering. De gemeente maakt contractuele afspraken met verwerkers, in zogenaamde verwerkersovereenkomsten.

Verder kan het voorkomen dat de gemeente samenwerkt met andere (overheids)organisaties om een taak van algemeen belang uit te voeren. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). De gemeente maakt ook met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Uitgangspunt is steeds dat derden een beschermingsniveau waarborgen dat gelijk is aan dat van de gemeente.

In het sociaal en veiligheidsdomein wordt ook samengewerkt met derden in samenwerkingsverbanden. Het doel is om vanuit verschillende perspectieven overzicht te creëren voor een effectieve aanpak bij een behoefte voor wmo- of jeugdhulp, meervoudige problemen bij personen, gezinnen, jongeren of individuen, die zorg mijden, overlast veroorzaken. Daarbij kan het wenselijk zijn persoonsgegevens van die personen tussen verschillende disciplines te delen om tot die effectieve aanpak te komen. Hierbij dient onderscheid te worden gemaakt in verwerking van persoonsgegevens tussen de verschillende afdelingen en teams binnen de gemeente en gegevensverwerking tussen de gemeenten en derden. Er zijn diverse samenwerkingsverbanden. De basis voor de gegevensverwerking is vaak uitgewerkt in afspraken over het kader waarbinnen de verwerking van persoonsgegevens plaatsvindt en hoe de rechten van betrokkenen zijn gewaarborgd. Deze methodiek blijft het uitgangspunt voor gegevensverwerking in samenwerkingsverbanden. Om te zorgen dat op een eenduidige manier vorm en inhoud aan deze afspraken wordt gegeven is een standaard protocol: 'Samenwerkingsverband integrale verwerking van persoonsgegevens opgesteld volgens het model convenant jeugdgroepaanpak van Ministerie van Justitie en Veiligheid, Politie, Openbaar Ministerie en de VNG. Zodra de Wet aanpak meervoudige problematiek sociaal domein in werking treedt zal bezien worden in hoeverre het modelconvenant hierop aangepast dient te worden.

Doorgifte buiten de EER

Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie, geschiedt alleen in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en dit privacybeleid.

Transparantie

De gemeente informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden.

De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Alleen als de wet anders bepaalt, wijkt de gemeente van deze informatieplicht af.

Rechten van betrokkenen

Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG uit te oefenen, te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid. Verzoeken van betrokkenen worden behandeld volgens het privacy protocol zoals bedoeld in onderdeel 3 van dit beleid.

Geschillenbeslechting

Als de betrokkene van mening is dat de gemeente niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij een klacht indienen middels de van toepassing zijnde klachtenprocedure zoals opgenomen in de privacyverklaring op de gemeentelijke website [Klacht indienen](#). De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

Verantwoording

Onder de verantwoordelijkheid van zowel het college van B&W als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de gemeente over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG intern wordt nageleefd. De gemeente stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.

De procesverantwoordelijken geven namens het college van B&W een verantwoording af over de wijze waarop zij persoonsgegevens verwerken bij het uitvoeren van (wettelijke) taken waar zij verantwoordelijk voor zijn. In het protocol is de verantwoordingsmethodiek uitgewerkt.

Verwerkingsregister

De gemeente beschikt over een verwerkingsregister, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt. Het verwerkingsregister is te raadplegen via de gemeentelijke website.

Gegevenseffectbeoordeling (GEB)

Als een verwerking mogelijk een hoog risico inhoudt, moet de gemeente een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. Dit is het geval als het om grootschalige verwerking van bijzondere persoonsgegevens gaat. De gemeente voert in dat geval een gegevenseffectbeoordeling (ook wel Data Processing Impact Assessment of DPIA genoemd). Als uit de GEB blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet de gemeente voldoende maatregelen nemen om de risico's te verminderen. Als het niet lukt om (voldoende) maatregelen te nemen om dit risico te beperken, dan moet de gemeente met de AP overleggen, voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd.

De gemeente beoordeelt het al dan niet uitvoeren van een GEB risicogestuurd. Dit kan betekenen dat procesverantwoordelijken namens het college tot het oordeel kunnen komen dat een verwerking waar mogelijk een hoog risico in verwerking van persoonsgegevens is geen GEB wordt uitgevoerd. De Privacy Officer en de CISO hebben daarbij een adviserende rol. De functionaris gegevensbescherming (FG) heeft hierbij een toezichthoudende rol. Het niet uitvoeren van GEB's bij mogelijke hoog risicoverwerkingen wordt op basis van draagkrachtige motivering gedocumenteerd door de procesverantwoordelijken. Bij het interne toezicht door FG geven de procesverantwoordelijken verantwoording af over hoog risicoverwerkingen waarvoor geen GEB is uitgevoerd. Dit kan eventueel betekenen dat als een niet ingeschat risico plaatsvindt, waarbij er sprake is van een hoog bestuurlijk afbreukrisico dat alsnog een DPIA wordt uitgevoerd.

Functionaris gegevensbescherming (FG)

De gemeente is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. De gemeente heeft daarom verplicht een FG aangesteld. De FG is de onafhankelijke intern toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG brengt jaarlijks een verslag uit aan de gemeenteraad en het College van B&W van zijn werkzaamheden, bevindingen en aanbevelingen.

PDCA Cyclus

De gemeente streeft ernaar om rondom de verwerking van persoonsgegevens *in control* te zijn en daarover op professionele wijze verantwoording af te leggen. *In control* betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus, die risicogestuurd is. In opdracht van de directie stellen de procesverantwoordelijken samen met de Privacy Office jaarlijks prioriteiten vast om privacymanagement te borgen en worden er afspraken gemaakt over de verantwoording van de uitgevoerde prioriteiten.

Daarnaast gebruikt de gemeente het borgingsproduct van de VNG als het beoordelingskader voor het waarborgen van privacy compliance binnen de gemeente. Het borgingsproduct geeft invulling aan het normenkader voor het duiden van privacy risico's en de daarbij behorende beheersmaatregelen binnen de gemeente Nieuwegein. Daarbij kan aanvullend ook CIP selfassessment worden toegepast. Het Centrum Informatiebeveiliging en Privacybescherming (CIP) heeft de Privacy Self Assessment (PriSA) opgesteld ter ondersteuning van het meten, verbeteren en bewaken van de privacy volwassenheid van organisaties.

Bewustwording

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de gemeentelijke organisatie voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd. Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies. Dit gebeurt passend binnen de context van en bij het domein waarbinnen die worden verwerkt.

Om het kennis- en toepassingsniveau van medewerkers over het veilig en bewust verwerken van persoonsgegevens bij het uitvoeren van hun werk te waarborgen past de gemeente een zogenaamde basiskennisrichtlijn toe die uitgewerkt wordt in specifieke modules. Dit gaat concreet om het ontwikkelen van leerlijnen voor basiskennis over o.a. de AVG en informatieveiligheid.

7. Intrekking oude beleidsregels

Het Beleidsplan veilig omgaan met persoonsgegevens in de gemeente Nieuwegein vastgesteld op 11 december 2018, wordt ingetrokken.

8. Geldigheidsduur

Dit beleid wordt tenminste een keer per vier jaar beoordeeld en zo nodig herzien. Als daar aanleiding toe is (bijvoorbeeld in geval van grote organisatorische veranderingen, wetswijzigingen, uitkomsten van DPIA's, o.i.d.) kan het college besluiten tot een tussentijdse aanpassing op onderdelen of een herziening.

9. Inwerkingtreding

Deze beleidsregels treden in werking met ingang van de dag na die van de bekendmaking.

10. Citeertitel

Dit beleid worden aangehaald als: Beleidsregels verwerking persoonsgegevens gemeente Nieuwegein 2026.

Aldus vastgesteld op 2 juni 2026

Ellie Liebregts
secretaris

Marijke van Beukering-Huijbregts
burgemeester