Privacybeleid voor de gemeente Nijmegen 2023

Privacybeleid gemeente Nijmegen 2023

De raad van de gemeente Nijmegen, bijeen in zijn vergadering van ….

Gelet op de Algemene verordening gegevensbescherming, de Uitvoeringswet Algemene verordening gegevensbescherming en de Wet Politiegegevens

Besluit

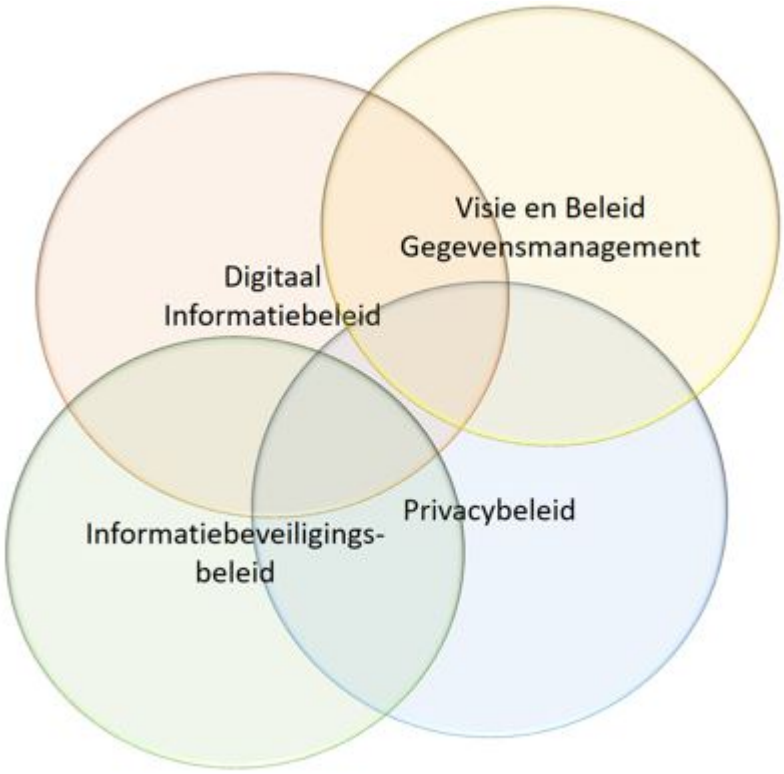
vast te stellen het Privacybeleid voor de gemeente Nijmegen 2023,

Inleiding

Sinds 2018 is de Algemene verordening gegevensbescherming (hierna: AVG) van kracht. Deze verordening bevat, samen met diverse verdragen en de Grondwet, de regels over de wijze waarop we met persoonsgegevens om dienen te gaan. De gemeente Nijmegen verwerkt persoonsgegevens voor diverse taken, zoals het verlenen van vergunningen en het verstrekken van uitkeringen. De burger moet er hierbij op kunnen vertrouwen dat de gemeente zorgvuldig en veilig met persoonsgegevens omgaat. Een verwerking van persoonsgegevens kan leiden tot privacyrisico's. Wanneer een verwerking niet gebeurt binnen de wettelijk gestelde kaders en er geen rekening wordt gehouden met proportionaliteit en subsidiariteit, kan het gebeuren dat er onrechtmatig of onnodig gegevens verwerkt worden.
Dit privacybeleid vervangt het eerder opgestelde privacybeleid uit 2018. De komst van de AVG was in 2018 een nieuw thema. Inmiddels zijn er vier jaren verstreken waar diverse lessen uit getrokken kunnen worden. Het privacybeleid is toe aan een update, waarin meer aandacht besteed is aan strategische componenten zoals visie en ambitie. Vanuit het beleidskader worden vervolgens meetbare doelen geformuleerd die mede zijn gestoeld op de jaarplannen van de Functionaris Gegevensbescherming (FG), de ENSIA audit en de BIO.
Gemeentelijk privacybeleid is van belang om op een formele wijze eenduidigheid binnen de organisatie te creëren op het gebied van het verwerken van persoonsgegevens. De visie die in dit beleid wordt gegeven is van toepassing op de hele gemeente. Verwerkingen van persoonsgegevens moeten op dezelfde wijze opgezet, geanalyseerd en beoordeeld worden. Bovendien draagt privacybeleid bij aan bewustwording van medewerkers van de gemeente en dient het als kader bij privacyvraagstukken.

Visie

1. Het respecteren van wettelijke kaders en de persoonlijke levenssfeer van de burgers.
   Als gemeente ontkomen wij niet aan het verwerken van persoonsgegevens. Een groot deel van onze taken zou onuitvoerbaar zijn zonder persoonsgegevens te verwerken. Ondanks dat het verwerken van persoonsgegevens een inbreuk kan maken op de persoonlijke levenssfeer van onze burgers, is het uitgangspunt hierbij dat we de persoonlijke levenssfeer van de burger zoveel mogelijk respecteren. We houden ons daarbij aan de wettelijke regels uit het gegevensbeschermingsrecht. Wij zien privacy als een belangrijke publieke waarde. Buiten de wettelijke kaders, verhoudt dit privacybeleid zich ook tot andere publieke waarden die zijn vastgelegd in ander informatiebeleid dat de gemeente hanteert. De afbeelding hieronder geeft deze verhoudingen weer.



2. Transparantie naar de burger
   Wij vinden het belangrijk om transparant te zijn over de wijze waarop wij omgaan met de gegevens van onze burgers. Het is voor de inwoners van onze stad belangrijk dat zij erop kunnen vertrouwen dat zorgvuldig met hun gegevens wordt omgegaan en dat hun gegevens op een veilige manier verwerkt worden. Daarom zijn we transparant over hoe we met persoonsgegevens omgaan. Een voorbeeld van deze transparantie is de publicatie van het verwerkingsregister op onze website. We informeren de gemeenteraad actief over onderwerpen rondom privacy, zodat er op een democratische wijze controle plaatsvindt op het handelen van de gemeentelijke organisatie met betrekking tot gegevensbescherming.
3. Belangrijk om persoonsgegevens goed te beschermen
   Privacy en informatiebeveiliging raken elkaar op verschillende vlakken. Eén van deze vlakken, is de bescherming van persoonsgegevens. Waar de AVG handvatten biedt over hoe om te gaan met persoonsgegevens, ziet informatiebeveiliging op de bescherming en beveiliging van alle gegevens. Zowel informatiebeveiliging als privacy vragen om een risico-gedreven aanpak. Het privacybeleid en informatiebeveiligingsbeleid dragen er aan bij dat er binnen de gemeente duidelijke richtlijnen zijn over hoe we omgaan met de bescherming van persoonsgegevens. Wij vinden het belangrijk dat dit op een uniforme wijze gebeurt zodat persoonsgegevens gemeentebreed en consequent goed beschermd worden.
4. Balans tussen dienstverlening en bescherming van persoonsgegevens
   Bij de verwerking van persoonsgegevens worden de wettelijke kaders uit de AVG, maar ook uit andere wetten, zoals de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) en de Wet Politiegegevens (WPG) gevolgd. Het volgen van deze kaders moet ertoe leiden dat er zorgvuldig met persoonsgegevens wordt omgegaan. Deze kaders zijn echter vrijwel nooit zwart-wit. Bij de verwerking van persoonsgegevens dient ook rekening te worden gehouden met dienstverlening aan de burger. Door de toenemende digitalisering van onze maatschappij wordt de snelheid van informatiestromen steeds groter. Dit betekent onder andere dat burgers, mogelijk via een digitale weg, op een juiste manier geholpen moeten kunnen worden bij vragen. De

wet biedt in veel gevallen de ruimte om rekening te houden met factoren zoals dienstverlening. Waar nodig willen we deze ruimte benutten. Hierbij houden we wel altijd rekening met proportionaliteit, subsidiariteit en noodzaak.

5. Aandacht voor de ethische component van privacy
   Persoonsgegevens moeten altijd verwerkt worden binnen de wettelijk gestelde kaders, anders is het onrechtmatig verwerking. Er moet ook gekeken worden of de verwerking wel verantwoord is om uit te voeren en van toegevoegde waarde is voor de maatschappij. Eén van die andere componenten is de ethische component. Als het verwerken van persoonsgegevens juridisch gezien is toegestaan, betekent dat niet per se dat het wenselijk is. Zo willen wij ook reflecteren op onze keuzes om bepaalde verwerkingen wel of juist niet uit te voeren. Sommige gegevensverwerkingen maken een (grote) impact op de maatschappij en dan spelen er extra afwegingen. Wij vinden het belangrijk dat deze afwegingen waar nodig op een juiste, onafhankelijke manier getoetst worden. Daarom hebben wij een onafhankelijke ethische commissie ingesteld. Deze commissie mag gevraagd of ongevraagd advies geven over de ethische aspecten van de verwerkingen van persoonsgegevens. Op deze manier willen we aan onze inwoners garanderen dat we onze keuzes niet alléén baseren op de wettelijke vereisten, maar dat we ook oog hebben voor de ethische kant.

Ambitie

Wij willen de privacy van onze inwoners zo goed mogelijk beschermen, zodat onze inwoners volledig kunnen vertrouwen op de wijze waarop wij met hun persoonsgegevens omgaan. Dit proberen we te bereiken door transparant te zijn over de manier waarop wij met gegevens omgaan. Dit sluit bovendien aan bij de uitgangspunten van het Manifest Open en Weerbaar. Om deze ambitie te bereiken, willen we realiseren dat in de komende vier jaar alle nodige beheersmaatregelen zijn vastgesteld (conform niveau 3 van de volwassenheidsstadia. Dat wil zeggen dat deze maatregelen zijn gedocumenteerd, gestructureerd en vastgesteld.
Het zogenaamde ‘Capability Maturity Model’ (CMM) – oftewel het Volwassenheidsniveau-model – is een algemeen gebruikt model dat aangeeft op welk volwassenheidsniveau de organisatie zit.

Capability Maturity Model

Niveau	Omschrijving
1. Ad-hoc	Beheersmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.
2. Beheerst	Beheersmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.
3. Vastgesteld	Beheersmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.
4. Voorspelbaar	De effectiviteit van de beheersmaatregelen wordt periodiek geëvalueerd.
5. Geoptimaliseerd	De beheersmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering.

Ter illustratie: een inwerkprocedure die voldoet aan niveau 3 is op papier vastgelegd en wordt bij elke nieuwe collega gevolgd. Hierdoor worden mogelijke maatregelen uit de inwerkinstructie omtrent privacy geborgd, waardoor de uitvoering aantoonbaar is en getoetst kan worden. In niveau 1 of 2 geschiedt de inwerkprocedure door collega’s die uitleg geven aan de hand van hun eigen gewoontes en niet aan de hand van een instructie. Hierdoor kunnen mogelijke (privacy)maatregelen niet worden getoetst.

Wij hebben de ambitie om zo snel mogelijk op privacygebied te voldoen aan volwassenheidsniveau 3; ‘Gedefinieerd proces’. Op dit niveau zijn processen gedocumenteerd en zijn betrokkenen bekend en vertrouwd met beleid,

richtlijnen en procedures. Op basis van niveau 3 is sprake van een volledige naleving van de AVG. Ook op andere thema's willen we dit niveau zo snel mogelijk halen, maar dat valt buiten de reikwijdte van dit beleid.
De beheersmaatregelen worden hieronder verder uitgewerkt, maar betekenen in ieder geval dat er meer aandacht komt voor werkinstructies, toepassingen van privacy by design en de benodigde onderleggers voor specifieke verwerkingen. Bovendien moet de uitvoering van deze beheersmaatregelen en documentatie met regelmaat getoetst worden. Meer specifiek betekent dit dat de benodigde aandacht besteed wordt aan de vereisten uit artikel 24, 25 en 35 AVG. In de alinea's hieronder wordt meer uitleg gegeven over de vereisten uit deze artikelen.

1. De juiste passende technische en organisatorische maatregelen treffen
   Als verwerkingsverantwoordelijke hebben wij een plicht om passende technische en organisatorische maatregelen te nemen die eraan bijdragen dat gegevensbeschermingsbeginselen zoals dataminimalisatie en transparantie maximaal nageleefd worden. Dat betekent meer concreet dat medewerkers met functies die daar om vragen een duidelijk omschreven werkinstructie moeten hebben waarin aandacht wordt besteed aan privacy en de aspecten die daarbij horen.
2. Privacy by design en privacy by default toepassen
   De beginselen van privacy by design en privacy by default worden waar mogelijk volledig toegepast. Hierbij blijft techniek natuurlijk voortdurend in ontwikkeling. Dat betekent dat er nieuwe mogelijkheden ontstaan die het makkelijker of beter mogelijk maken om de gegevensbeschermingsbeginselen op een gestandaardiseerde manier toe te passen. Wanneer de techniek nog achterblijft en privacy by design geen optie is, worden in ieder geval de passende technische en organisatorische maatregelen getroffen om ervoor te zorgen dat er enkel persoonsgegevens worden verwerkt die noodzakelijk zijn voor het specifieke doel. De toepassing van privacy by design wordt bij de uitgangspunten voor gemeentelijk handelen verder toegelicht.
3. DPIA's hebben voor alle verwerkingen met een mogelijk hoog risico
   Sinds de invoering van de AVG geldt het vereiste dat verwerkingen van persoonsgegevens met mogelijk hoge risico's onderlegd moeten worden met zogeheten Data Privacy Impact Assessments (DPIA). De afgelopen jaren hebben we grote stappen gezet in de uitvoering van DPIA's. Het is echter zo dat alle verwerkingen met een mogelijk hoog risico een DPIA vereisen als onderlegger. Het is onze ambitie om zo snel mogelijk alle benodigde DPIA's gereed te hebben. Hierbij proberen we de verwerkingen met de hoogste risico's met prioriteit op te pakken.
4. Inzetten op het privacybewustzijn van onze medewerkers
   Het vergroten van het privacybewustzijn onder medewerkers is een essentieel onderdeel om aan de gemeentelijke privacyambities te voldoen. Dit bewustzijn zorgt er voor dat medewerkers begrijpen wat de gemeentelijke richtlijnen zijn over hoe zij met persoonsgegevens om moeten gaan, maar ook dat zij weten wanneer er bijvoorbeeld een DPIA uitgevoerd moet worden. Overigens draagt het maken van een DPIA ook bij aan het vergroten van het privacybewustzijn en heeft het dus een zelfversterkend effect. Omdat dit een dermate essentieel onderdeel is van de strategie om een meer privacyvriendelijke organisatie te worden zetten we onder andere in op privacycampagnes en e-learnings.

Uitgangspunten gemeentelijk handelen

De visie en ambitie die in dit beleid worden genoemd, zijn gestoeld op een aantal uitgangspunten die wij aanhouden voor gemeentelijk handelen. Deze uitgangspunten zijn hieronder uitgewerkt.
Privacy by design
Privacy by design wil zeggen dat bij de inrichting van nieuwe diensten of producten op een juiste manier rekening wordt gehouden met privacyaspecten. Het is, naast een wettelijke verplichting, het uitgangspunt op basis waarvan gegevensverwerkingen worden ontworpen. Een goede inbedding van privacy by design is cruciaal om invulling te geven aan privacymanagement. Om de toepassing van privacy by design te maximaliseren, hanteren wij het 'pas toe, of leg uit' principe. Dat wil zeggen dat het uitgangspunt is dat privacy by design wordt toegepast en wanneer dat we

dat niet doen, dat we toelichten waarom. Om de toepassing van privacy by design structureel in te bedden in onze organisatie, is het noodzakelijk dat wij voorafgaand aan een nieuwe gegevensverwerking of bij de aanschaf van een nieuwe applicatie, nadenken over een inrichting die de privacy van betrokkenen zo goed mogelijk waarborgt. Concreet gezien verstaan wij onder een goede toepassing van privacy by design dat er met acht verschillende principes rekening wordt gehouden. De principes zijn opgedeeld in twee hoofdgroepen: de data-georiënteerde principes, en de procesgeoriënteerde principes.

Data-georiënteerde strategieën

Deze strategieën zijn technisch van aard en richten zich op de verwerkingen van de gegevens zelf.

- minimaliseer: beperk de verwerking van persoonsgegevens waar dat kan.
- scheid: scheid de verwerking veel mogelijk van elkaar.
- abstraheer: beperk het detail waarin persoonsgegevens worden verwerkt.
- verberg: bescherm persoonsgegevens, of maak ze onherleidbaar of onobserveerbaar.

Procesgeoriënteerde strategieën

Deze strategieën zijn organisatorisch van aard en richten zich op de processen rondom de verwerkingen van persoonsgegevens.

- informeer: informeer personen tijdig over de verwerking van hun persoonsgegevens.
- geef controle: geef personen waar mogelijk controle over de verwerking van hun persoonsgegevens.
- dwing af: verbind je aan een privacyvriendelijke verwerking van persoonsgegevens, en dwing deze af.
- toon aan: toon aan dat je op een privacyvriendelijke wijze persoonsgegevens verwerkt.

Integriteit

Wij gaan op een veilige, professionele en integere wijze met persoonsgegevens om. De privacy van betrokkenen wordt gerespecteerd en het nemen van besluiten op basis van geautomatiseerde systemen is mede op basis van het Digitaal informatiebeleid niet toegestaan. Ambtenaren gebruiken de persoonsgegevens waarover zij beschikken in het kader van de uitoefening van hun functie, enkel voor de uitoefening van deze functie, in ieder geval wanneer deze gegevens niet openbaar zijn. Bovendien beschermt de medewerker deze informatie door de bestaande voorschriften, zoals de relevante wettelijke kaders en werkafspraken, te volgen.

Bewust omgaan met persoonsgegevens

Een medewerker moet zich bij de uitoefening van zijn/haar taken voortdurend bewust zijn van het belang van privacy. Om bewustwording te realiseren is verplichte kennisdeling over het onderwerp noodzakelijk. Het GMT zorgt er samen met de in dit beleid genoemde functionarissen voor dat de informatie over informatiebeveiliging en gegevensbescherming herhaaldelijk onder de aandacht wordt gebracht bij de medewerkers.

Doelbinding, proportionaliteit en subsidiariteit

Persoonsgegevens worden alleen verzameld voor een van te voren bepaald en concreet omschreven doel. Hierover is de gemeente transparant naar de burgers, zoals te zien in ons verwerkingsregister op www.nijmegen.nl. Het vooraf bepaalde doel bepaalt ook de omvang en de reikwijdte van de te verwerken persoonsgegevens. Het uitgangspunt is dan ook dat niet meer persoonsgegevens worden verzameld of verwerkt dan noodzakelijk is. Daarnaast gelden de uitgangspunten dat de verzameling van persoonsgegevens in verhouding met moet staan tot het doel waarvoor ze worden verzameld (dit noemen we het proportionaliteitsbeginsel) en dat persoonsgegevens worden verzameld op een wijze die zo min mogelijk inbreuk maakt op de privacy (dit noemen we het subsidiariteitsbeginsel).

Transparantie

Wij zijn transparant over de verwerking van persoonsgegevens. Via het register van verwerkingen en de privacyverklaring op de website is algemene informatie over privacy, contactgegevens van de FG, doelen en grondslagen te vinden. Daarnaast geven wij bij alle gegevensverwerkingen aanvullende informatie over de specifieke gegevensverwerking.

Delen met (interne) derden.

Bij doorgifte van basisregistraties met externe partijen of tussen afdelingen waarbij sprake is van verwerking van persoonsgegevens, maken we afspraken over de eisen van gegevensuitwisseling. Deze afspraken worden vastgelegd in een gegevensleveringsovereenkomst.
Hierdoor wordt de zorgvuldige omgang met persoonsgegevens op een herleidbare wijze geborgd.

Data Protection Impact Assessment, DPIA

Een DPIA ofwel gegevensbeschermingseffectbeoordeling zorgt ervoor dat de (medewerkers van) de gemeente stil staan bij de effecten en risico's van nieuwe, gewijzigde of bestaande verwerkingen op de juistheid van de verwerking van persoonsgegevens en de beveiliging ervan. Een DPIA is verplicht bij een risicovolle verwerking of op verwerkingen die mogelijk een verhoogd risico opleveren. De gemeente voert deze in ieder geval uit als er sprake is van een verwerking die voldoet aan de criteria van een risicovolle verwerking of als bijzondere persoonsgegevens worden verwerkt. Dit geldt in ieder geval bij de toepassing van nieuwe technologieën.
Voor alle verwerkingen wordt advies gevraagd aan de Privacy Officer, een andere jurist of een I-adviseur over het uitvoeren van een DPIA. Niet alleen voorafgaand aan het uitvoeren van de verwerking, maar ook over het uitvoeren van een DPIA alsmede over de uit de DPIA voortgekomen maatregelen. Een DPIA wordt tijdig uitgevoerd. Dit betekent in ieder geval voordat de verwerking start of voordat de wijziging van een verwerking operationeel wordt. De uit de DPIA voortvloeiende maatregelen om risico's te minimaliseren worden tijdig en na definitief advies van de Functionaris voor de gegevensbescherming geïmplementeerd.

Doorgifte buiten de EU/ EER

Binnen de EU gelden dezelfde regels voor het beschermen van persoonsgegevens en mogen persoonsgegevens doorgegeven en verwerkt worden. Wij geven in principe geen persoonsgegevens door buiten de EU. Als dit toch onvermijdelijk of noodzakelijk is, dan is er een aanvullende maatregel vereist, zoals een adequaatheidsbesluit of een modelcontract. Wij vereisen een passend beschermingsniveau en maken een afweging volgens een vastgestelde risicomatrix.

Persoonsgegevens moeten juist zijn

Wij hebben een actieve onderzoeksplicht als het aankomt op de juistheid van persoonsgegevens. Waar nodig dienen we de gegevens te actualiseren en actueel te houden. Bovendien kan een burger, indien persoonsgegevens onjuist zijn, ons vragen dit aan te passen.

Technologie

Door de technologische vooruitgang worden steeds meer apparaten en voorzieningen die wij gebruiken 'slim'. Deze apparaten en voorzieningen verzamelen data en zijn daarbij in staat om al deze persoonsgegevens, apparaten en voorzieningen met elkaar te verbinden. Waar het een oplossing biedt passen we nieuwe technologische ontwikkelingen toe ter ondersteuning van onze processen. Dit doen wij altijd binnen kaders van de wet, met inachtneming van de ethische aspecten en met toepassing van de acht strategieën van privacy by design.
Met deze nieuwe technieken is het mogelijk om aan profilering te doen. Wij verstaan onder profilering het aan de hand van een geautomatiseerde verwerking van meerdere persoonsgegevens selecteren van personen die aan bepaalde van te voren gestelde (risico)criteria voldoen. In Nijmegen is er nooit sprake van besluitvorming op basis van profilering zonder menselijke tussenkomst.

Inzet van camera's

Wij kunnen in bepaalde omstandigheden cameratoezicht inzetten, zoals vastgelegd in de Gemeentewet, op basis van verkeerswetgeving of op basis van de AVG bij een gerechtvaardigd organisatiebelang. Cameratoezicht kan onder andere worden gebruikt voor het vergroten van de veiligheid op straat. Camera's kunnen een grote inbreuk maken op de privacy van diegenen die gefilmd worden. Om de privacy zo goed mogelijk te waarborgen worden camera's alleen ingezet wanneer er geen andere manieren zijn om het doel te bereiken en worden er eisen gesteld aan de inzet van camera's. Camera's in de publieke ruimte vinden hun grondslag in de Gemeentewet. Op belangrijke A-doorstroomwegen hangen Incidentmanagement camera's. Tenslotte hangen er camera's rondom en in publiek toegankelijke ruimten van de dienstpanden en in de parkeergarages en bij de roadbarriers vanuit een gerechtvaardigd belang.

De BOA's werkzaam bij de gemeente Nijmegen zijn sinds begin 2018 uitgerust met bodycams. De bodycam wordt gebruikt om bij eventuele incidenten een de-escalerend effect teweeg te brengen, maar is wel aan strikte regels gebonden. Hiervoor hebben wij het 'Uitwerkingsbesluit betreffende de inzet van Bodycams' opgesteld.

Wet open overheid (Woo)

Via de Wet open overheid (Woo) kan een verzoek om informatie worden ingediend. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In beginsel worden geen persoonsgegevens verstrekt.

Wet hergebruik van overheidsinformatie

De Wet hergebruik van overheidsinformatie regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek wordt altijd getoetst of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In beginsel worden geen persoonsgegevens verstrekt.

Wet Politiegegevens

De wet Politiegegevens stelt de kaders voor hoe omgegaan moet worden met politiegegevens. Hoewel het grote merendeel van de persoonsgegevens die binnen de gemeente worden verwerkt, vallen onder de AVG, werken we ook met politiegegevens. De bijzondere opsporingsambtenaren (boa) werken naast persoonsgegevens, ook met politiegegevens. Hiervoor moeten zij dus werken met zowel de kaders van de AVG, als die van de WPG. Bovendien moet het duidelijk zijn voor de boa welke gegevens onder welke wet vallen.

Onderstaande verplichtingen volgen specifieke uit de WPG. Wij volgen deze verplichtingen en borgen deze in de desbetreffende 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.

Een andere verplichting uit de WPG is het uitvoeren van externe audits op het gebied van de WPG. De rapportage die hieruit voortvloeit moet worden verstrekt aan de AP. Als er tekortkomingen zijn geconstateerd moet 3 maanden na het uitvoeren van de audit een verbeterrapport worden opgesteld, waarop binnen een jaar een hercontrole plaatsvindt. 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.

Rechten van betrokkenen

Wij honoreren de rechten van burgers zoals vastgelegd in de Algemene verordening gegevensbescherming. Wij hebben de rechten van betrokkenen waar mogelijk geïmplementeerd in onze processen en helpen de betrokkene zo gericht mogelijk. Bovendien wordt gewerkt aan de 'Mijn Nijmegen'-omgeving, waar burgers hun eigen gegevens bekend bij de gemeente zelf in kunnen zien.

Rollen en verantwoordelijkheden

Binnen de gemeente Nijmegen zijn verschillende rollen en verantwoordelijkheden belegd om uitvoering te geven aan het privacybeleid.

Gemeenteraad

De gemeenteraad stelt de kaders en uitgangspunten rondom privacy vast. De gemeenteraad controleert of college van B&W zich houdt aan deze kaders.

College van B&W

Het college van B&W is verantwoordelijk voor het verwerken van persoonsgegevens binnen de gestelde kaders. Het college stelt hiervoor de beleidskaders en specifieke regelingen en procedures vast. Jaarlijks legt ze verantwoording af aan de gemeenteraad over privacy en de toepassing van het privacybeleid in de ENSIA rapportage en via de Auditcommissie.

Het Gemeentelijk Management Team (GMT) en de Concernmanagers

Het GMT en de concernmanagers zijn verantwoordelijk voor het sturen op en monitoren van de uitvoering van het beleid. Ze stimuleren bewustwording over privacy bij medewerkers. Tevens zijn de concernmanagers verantwoordelijk voor het vaststellen van doelen en middelen om persoonsgegevens te verwerken, bijvoorbeeld door het uitvoeren van een Data Protection Impact Assessment (DPIA). De Concernmanagers zijn tevens verantwoordelijk voor het afhandelen en melden van datalekken binnen hun afdeling.

Directie

De directie is verantwoordelijk voor het sturen op en monitoren van de uitvoering van het beleid op organisatieniveau.

Gemeentesecretaris

De Gemeentesecretaris is de voorzitter van het gemeentelijk crisisteam wat bij elkaar komt bij een I-crisis.
Door het activeren van het I-crisisprotocol verkrijgt de Gemeentesecretaris het mandaat om op basis van advies van het gemeentelijk crisisteam, een opdracht aan het iRvN te formuleren om bijvoorbeeld dienstverlening (deels) stil te leggen bij een groot datalek.

Functionaris voor de gegevensbescherming (FG)

De Functionaris voor de gegevensbescherming is verantwoordelijk voor het intern onafhankelijk toezicht op en adviseren van de organisatie over de juiste en zorgvuldige omgang met persoonsgegevens vanuit een derdelijns rol. Hierbij kan de Functionaris voor de gegevensbescherming rechtstreeks de Autoriteit Persoonsgegevens inschakelen. De Autoriteit Persoonsgegevens kan ook uit eigen beweging een onderzoek doen naar de naleving van de privacywetgeving. Daarnaast kan de Autoriteit Persoonsgegevens op verzoek van belanghebbenden (zoals burgers of belangenorganisaties) een onderzoek instellen. De FG heeft een wettelijke toezichthoudende taak. Om die reden kan en mag hij zich niet met de dagelijkse uitvoerende privacywerkzaamheden bezighouden. Dit is gescheiden.

Privacy Officer (PO)

De Privacy Officer is belast met de dagelijkse werkzaamheden. De functie PO is geen formele functie, maar de werknaam voor de juridische functionaris die zich bezighoudt met strategische en adviserende, controlerende en uitvoerende privacywerkzaamheden op organisatieniveau. Het college van B&W stelt in een besluit vast wie de rol van PO vervult. Daarmee is het voor de organisatie duidelijk wie het tweedelijns aanspreekpunt is voor alle privacyvraagstukken.

Chief Information Security Officer (CISO)

De CISO ondersteunt, coördineert en adviseert vanuit een onafhankelijke positie over de te nemen maatregelen voor informatiebeveiliging. Hij of zij rapporteert hierover aan het bestuur, de directie en het Gemeentelijk Management Team.

Security Officer (SO)

De SO is op de hoogte van de risico's en dreigingen voor de gemeente op tactisch niveau en ondersteunt bij het behalen van informatiebeveiligingsdoelstellingen. Hij of zij adviseert bovendien medewerkers op casusniveau over informatiebeveiliging en ondersteunt het programma voor security awareness.

Chief Information Officer (CIO)

De CIO is op de hoogte van nieuwe ontwikkelingen op ICT-gebied voor de gemeente en draagt zorg voor een strategische visie op informatievoorzieningen en rapporteert hierover aan het Gemeentelijk Management Team. Hij of zij is daarnaast opdrachtgever en aanspreekpunt van IRvN.

Privacy ambassadeurs

De privacy ambassadeur onderschrijft het belang van privacy en ondersteunt collega's bij het naleven van de regels die hiervoor binnen de organisatie zijn opgesteld. De ambassadeur is het eerste aanspreekpunt binnen de afdeling en spreekt collega's laagdrempelig aan waar nodig. De ambassadeurs helpen om maatregelen collectief aanvaardbaar te maken. Elke afdeling heeft minimaal één privacyambassadeur. Afdelingen die op een grootschalige wijze persoonsgegevens verwerken hebben één privacyambassadeur per bureau.

Medewerkers

Alle medewerkers (inclusief inhuur/externen) zijn verantwoordelijk voor de bescherming van de privacy van burgers en collega's. Dat betekent dat iedereen zorgt, binnen de kaders van zijn rol/functie, voor een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens en bewust is van de zorgvuldige verwerking hiervan.

Autoriteit Persoonsgegevens (AP)

De Autoriteit Persoonsgegevens is de landelijk aanwezen toezichthoudende instantie.

Sturing en monitoring

We hebben een aantal (vaak wettelijk voorgeschreven) instrumenten geïmplementeerd om de beginselen rondom privacy en gegevensbescherming vast te leggen. Dit zijn in ieder geval de DPIA's, de verwerkersovereenkomsten en de privacy protocollen. Allen hebben een eigen werking en bedoeling (zie omschrijving in de bijlage).

Het opstellen en vormgeven van deze instrumenten is al een interventie op zich wat betreft privacybewustzijn en privacybescherming.

Het naleven van de afspraken die vastgelegd zijn in deze instrumenten, is een volgende stap.

Voor het toetsen van de naleving gebruiken we het kader van de Tafel van 11 (Instrument ontwikkeld door het Expertise centrum Rechtspleging en Rechtshandhaving van ministerie van Justitie).

Dit kader kent twee dimensies: spontane naleving en handhaving.

Spontane naleving is intrinsiek. Dat betekent dat mensen de regels en afspraken naleven omdat ze het doel, de werking en het effect ondersteunen. Handhaving is vaak tijdens de uitvoering of ná de uitvoering en is een vorm van dwang.

In het controlplan van de FG worden beide dimensies gehanteerd. Hierbij starten we met 'spontane naleving', uitgaande van de verantwoordelijkheid van de eigen organisatie en haar management.

Vanuit de FG rol wordt toegezien op de naleving. Eens per jaar wordt de gemeentelijke organisatie bevraagd door de FG over de uitvoering van deze naleving. Zij dient dit 'evidenced based' (met acties en documenten onderbouwd) aan te geven. Dit controlemoment is tevens een uiting van handhaving tijdens de uitvoering: op basis van de bevindingen en aanbevelingen van de FG, kan er tijdens de uitvoering door het GMT bijgestuurd worden.

Eens per jaar maakt de FG een jaarverslag waarin de stand van zaken met betrekking tot de uitvoering van de privacybeginselen wordt weergegeven.

Inwerkingtreding

De inwerkingtreding van deze beleidsregels is op de dag na publicatie in het Gemeenteblad. Onder intrekking van het privacybeleid 2018

Aldus vastgesteld in de openbare raadsvergadering van:

De raadsgriffier,

Drs. S.J. Ruta

De voorzitter,

Drs. H.M.F. Bruls

Bijlage 1 Wettelijke kaders voor de verwerking en omgang met persoonsgegevens

Het college van Burgemeester en Wethouders is verantwoordelijk voor het integraal opstellen, en uitvoeren van het onderhavige privacybeleid. Hiervoor is dit beleid in lijn met, of sluit aan op de actualiteiten van:

- de Algemene verordening gegevensbescherming;
- de Uitvoeringswet Algemene verordening gegevensbescherming;
- Wet Politiegegevens;
- het Informatiebeveiligingsbeleid welke is vastgesteld door het college van Burgemeester en Wethouders;
- Strategisch informatiebeleid welke vastgesteld door het college van Burgemeester en Wethouders;
- Het Privacyreglement voor de gemeente Nijmegen;
- Code voor Informatiebeveiliging (NEN/ISO 27002);
- Baseline Informatiebeveiliging Overheid.

Bijlage 2 Begrippenlijst

Adequaatheidsbesluit
De AVG is geldend recht binnen de Europese Unie. Buiten de Europese Unie, kunnen dus andere veiligheidsmaatregelen gelden. Als er een adequaatheidsbesluit van kracht is tussen de EU en een land daarbuiten, betekent dat dat persoonsgegevens gedeeld mogen worden, zonder aanvullende voorwaarden te treffen.

Dataminimalisatie
Door niet meer gegevens te verzamelen dan noodzakelijk, voldoe je aan dataminimalisatie.

DPIA
Een DPIA is een risicoanalyse die wordt uitgevoerd op gegevensverwerkingen met een mogelijk hoog risico. Het maken van een DPIA levert inzichten op over hoe en waarom je een bepaalde verwerking doet en of het op een meer privacyvriendelijke manier kan. Daarnaast geeft het de risico's van bepaalde verwerkingen weer.

Modelcontract
Wanneer een partij uit de EU persoonsgegevens wil delen met een partij buiten de EU en er is geen adequaatheidsbesluit tussen het betreffende land en de EU, dan kan een modelcontract gelden als aanvullende maatregel, zodat de verwerking toch mogelijk wordt gemaakt. In een modelcontract worden aanvullende afspraken gemaakt over de beveiliging van persoonsgegevens.

Privacy by default

Wanneer privacy by design (zie hieronder) niet mogelijk is omdat de inrichting van een systeem al is gedaan, kun je privacy by default toepassen. Dat is de technische maatregelen treffen die naar de mogelijkheden van de inrichting ervoor zorgen dat privacy zo goed mogelijk beschermd wordt.

Privacy by design
Bij de inrichting van een bepaalde gegevensverwerking rekening houden met aspecten van privacy, zodat de inrichting geschiedt op een manier die zo privacyvriendelijk mogelijk is.

Proportionaliteit
Om te bepalen of een verwerking noodzakelijk is, moet ook proportionaliteit bepaald worden. Proportionaliteit gaat over de afweging van de inbreuk op de privacy, ten opzichte van het doel dat de verwerking moet bereiking. Als dit doel in juiste verhouding staat met de inbreuk op privacy, is de verwerking proportioneel.

Subsidiariteit
Om te bepalen of een verwerking noodzakelijk is, moet ook subsidiariteit bepaald worden. Dit gaat over of het doel van de verwerking bereikt kan worden met minder gegevens. Als dat niet zo is, dus als je niet meer uitvraagt dan noodzakelijk, is de verwerking subsidiair.