

Algemeen Privacyreglement

Het college van Burgemeester en Wethouders,
In zijn vergadering van 7 mei 2019,
Gezien het voorstel met reg.nr. 8906254,

overwegende dat het Algemeen Privacyreglement een uitwerking vormt van de Algemene Verordening Gegevensbescherming (AVG) en een praktische handleiding voor de organisatie; de regels en uitgangspunten geeft voor de eerlijke, zorgvuldige en rechtmatige verwerking van persoonsgegevens,

B E S L U I T:

het Algemeen Privacyreglement vast te stellen.

Algemeen Privacyreglement

In dit reglement laat de gemeente 's-Hertogenbosch zien op welke manier zij dagelijks omgaat met persoonsgegevens en privacy. Hierbij is ook de nadruk met het oog op wat er wettelijk wel en niet verantwoord is. Privacy speelt een belangrijke rol in de relatie tussen de inwoner en de overheid en staat daarmee hoog op de bestuurlijke agenda. Als gemeente zijn we verplicht om zorgvuldig en veilig, proportioneel en betrouwbaar om te gaan met de persoonsgegevens van inwoners. Dat geldt dus ook voor taken op het gebied van de basisadministraties, openbare orde en veiligheid en het sociaal domein. Ook willen wij als werkgever goed om gaan met de persoonsgegevens van onze ambtenaren en medewerkers. Deze regels zijn apart uitgewerkt in hoofdstuk 29 van de Rechtspositieregeling en in het privacyreglement medewerkers. Het beschermen van privacy wordt steeds complexer door technologische ontwikkelingen, de decentralisaties, grote uitdagingen op het terrein van veiligheid en door nieuwe Europese wetgeving. Daarom vinden wij het belangrijk om transparant te zijn over de manier waarop wij met persoonsgegevens en privacy omgaan.

1. De Bossche aanpak

De Gemeente 's-Hertogenbosch respecteert en beschermt de privacy en persoonsgegevens van haar inwoners. In de uitoefening van haar publiekrechtelijke taak houdt zij zich aan de wet en zoekt waar mogelijk de ruimte om de privacybelangen van zowel de inwoner als de doelstellingen van de gemeente naar beste inzicht te behartigen. Het is daarom belangrijk dat onze medewerkers privacy bewust zijn. De gemeente wil hiermee aantonen dat wij beschikken over medewerkers die bewust zijn van de risico's bij het werken met persoonsgegevens. Om privacy bewust te worden zorgt de gemeente voor kennissessies en workshops op het gebied van privacy en het omgaan met persoonsgegevens. Ook volgt iedere medewerker periodiek een e-learning waarmee naast kennisoverdracht ook de aanwezige privacy kennis wordt gemeten. Ook stelt de gemeente diverse handleidingen, factsheets en overige materialen ter beschikking om de medewerker handvatten te bieden bij het verwerken van de persoonsgegevens waarmee zij werken.

2. Wetgeving en definities

De Algemene Verordening Gegevensbescherming (AVG) en uitvoeringswet AVG (UAVG) regelen, sinds 25 mei 2018, het juridische kader voor de omgang met persoonsgegevens in Nederland. Begrippen uit de AVG en de UAVG die in dit Algemeen Privacyreglement worden gebruikt, hebben dezelfde betekenis.

Overige wetgeving om in het bijzonder rekening mee te houden:

Wet basisregistratie Personen: Het wettelijk kader van de AVG en UAVG, ziet niet op de specifieke verwerkingen die wij als gemeente verrichten in het kader van de uitvoering van de basisregistratie personen (BRP). Hiervoor is de Wet BRP van toepassing.

Wet openbaarheid van bestuur (Wob): Via de Wob (en straks wellicht de Wet Open Overheid) kun je een verzoek om informatie indienen bij de gemeente. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe 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 bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

3. Reikwijdte

Het Algemeen Privacyreglement is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van de gemeente. Oftewel: voor alle verwerkingen die binnen de gemeente plaatsvinden. Dit Algemeen Privacyreglement vormt een verdere uitwerking van de wettelijke regelgeving en een praktische handleiding voor de organisatie. Het geeft de regels en uitgangspunten voor de eerlijke, zorgvuldige en rechtmatige verwerking van persoonsgegevens.

4. Verantwoordelijke voor de verwerking

De bestuursorganen van de gemeente zijn allemaal verantwoordelijken voor de verwerkingen die door of namens de gemeente worden uitgevoerd. De bestuursorganen van de gemeente zijn onder andere de burgemeester, het college van Burgemeesters en Wethouders (college van B&W) en de Raad.

5. Verwerkingen

Wij verwerken persoonsgegevens om onze wettelijke taken uit te voeren en om diensten te verlenen aan inwoners en bedrijven. Het gaat dan bijvoorbeeld om de processen binnen het sociaal domein, zoals het beoordelen van een uitkering, wmo- of jeugdwetvoorziening. Maar ook het afhandelen van vergunningaanvragen, het innen van de gemeentelijke belastingen, het bijhouden van de Basisregistratie Personen of bij het toezien op de openbare orde en veiligheid. In al deze gevallen verwerken wij persoonsgegevens van inwoners en andere betrokkenen.

6. Doeleinden

Algemeen uitgangspunt is dat persoonsgegevens alleen verwerkt mogen worden als daarvoor een doel bestaat. Dit doel moet welbepaald, duidelijk omschreven en gerechtvaardigd zijn. De verwerkingsdoelen zijn het 'waarom' van het verwerken van persoonsgegevens. Doelen zijn van belang voor verschillende normen. Denk hierbij aan het bepalen wie verantwoordelijk is voor de verwerking van persoonsgegevens. Of de vraag of het delen van persoonsgegevens met andere organisaties is toegestaan. Ook zijn doelen van belang voor het vaststellen van bewaartermijnen en het informeren van de inwoner. Zo weten we hoe lang we persoonsgegevens mogen bewaren of waar we de inwoners over moeten informeren.

Ook moet steeds nagaan worden of het verwerken van persoonsgegevens noodzakelijk is voor het doel. Voor de uitvoering van diverse wetten zal in die wet vaak zijn aangegeven welke persoonsgegevens nodig zijn en dus verwerkt mogen worden. Voorbeelden hier van zijn de Participatiewet en de Jeugdwet. Daar waar over verwerking van persoonsgegevens in bijzondere wetgeving niets is geregeld, gelden de algemene regels van de AVG en de UAVG.

Een belangrijke eis is dat de doelen niet te ruim en vaag omschreven mogen zijn of achteraf bepaald worden. De persoonsgegevens mogen daarnaast in principe niet gebruikt worden voor een ander doel dan waarvoor deze zijn verzameld. Voor verwerking voor een andere doel is opnieuw een rechtsgrond nodig. Ook moet er opnieuw aan de AVG en UAVG voldaan worden. Verwerking voor een ander doel dan het oorspronkelijke doel is alleen onder strikte voorwaarden toegestaan. Zo zal er een directe relatie moeten zijn met het doel waarvoor de persoonsgegevens eerder zijn verzameld. Algemeen geldt: hoe gevoeliger het persoonsgegeven, hoe minder snel er aangenomen mag worden dat er sprake is van verenigbaar gebruik. Ook moet men rekening houden met de gevolgen van de beoogde verwerking voor de betrokkene. Denk hierbij aan het vooraf inlichten van de inwoners over het doel waarvoor de gegevens worden gebruikt als de inwoner zijn persoonsgegevens aan de gemeente geeft. Bijvoorbeeld voor de aanvraag van een parkeer- of bouwvergunning. Wel zijn er enkele uitzonderingen voor het hergebruiken van persoonsgegevens voor andere doelen. Een voorbeeld hiervan is het hergebruiken van persoonsgegevens voor wetenschappelijk onderzoek en statistiek.

7. Noodzakelijkheid

Voor alle grondslagen, met uitzondering van het nakomen van een wettelijke plicht, zal altijd gemotiveerd moeten worden waarom de verwerking van persoonsgegevens noodzakelijk is om het doel te bereiken. Hierbij zal moeten worden afgewogen of het verwerken van bepaalde persoonsgegevens in verhouding staat tot het doel wat we willen bereiken. Daarnaast zal moeten worden overwogen of het doel ook op een ander wijze, dus zonder die persoonsgegevens, bereikt kan worden.

8. Rechtmatige grondslag

8.1 Wettelijke grondslagen en algemene uitgangspunten

Voor elke verwerking van persoonsgegevens moet er een rechtmatige grondslag van toepassing zijn. Iedere verwerking van persoonsgegevens moet gebaseerd worden op één van de volgende zes grondslagen:

- a. de betrokkene heeft voor de verwerking zijn ondubbelzinnige toestemming verleend;
- b. de gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, waarbij ook rekening moet worden gehouden met de precontractuele fase;
- c. de gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen;
- d. de gegevensverwerking is noodzakelijk voor een vitaal belang van de betrokkene (in het kader van leven of dood, bijvoorbeeld delen van gegevens bij opname spoedeisende hulp);
- e. de gegevensverwerking is noodzakelijk voor vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
- f. de gegevensverwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de gemeente of van een derde aan wie de gegevens worden verstrekt. Maar als het belang op bescherming van zijn privacy voor de betrokkene zwaarder weegt, dan is de rechtsgrond gerechtvaardigd belang niet van toepassing.

Van de zes grondslagen zijn voor de gemeente in de praktijk de wettelijke plicht en de goede vervulling van taak van algemeen belang of openbaar gezag leidend. Voor de interne bedrijfsvoering van de gemeente, voor de medewerkers dus, spelen ook de grondslagen gerechtvaardigd belang en de uitvoering van een overeenkomst een rol. Het gerechtvaardigd belang mag nooit als reden worden gebruikt voor de verwerking van gegevens voor een publiekrechtelijke taak.

8.2 Toestemming

8.2.1 Toestemming als grondslag in de zin van de AVG

Wordt de grondslag toestemming gebruikt, dan is de betrokkene vooraf geïnformeerd over het volgende:

- waarvoor de toestemming gevraagd wordt;
- waarom de toestemming noodzakelijk is;
- op welke instanties of personen de uitwisseling betrekking heeft
- welke informatie/persoonsgegevens uitgewisseld gaan worden
- bij welke partijen de informatie verzameld wordt
- en met welke partijen die gegevens dan uitgewisseld worden
- zijn of haar recht om de toestemming weer in te trekken en de mogelijke gevolgen daarvan

Toestemming is alleen een rechtmatige grondslag wanneer deze vrij, geïnformeerd, actief en ondubbelzinnig is. De inwoner kan voor veel voorzieningen enkel aankloppen bij de eigen gemeente. Daarmee is de inwoner dus afhankelijk van de gemeente. Als er dus een afhankelijkheidsrelatie bestaat tussen de gemeente en de inwoner, dan zal de grondslag toestemming zelden 'vrij gegeven' zijn. Alleen in uitzonderlijke situaties is toestemming van de inwoner een rechtmatige grondslag. Toestemming wordt vastgelegd op een daarvoor bedoelde formulier en genoteerd in het dossier.

8.2.2 Andere vormen van toestemming

Toestemming kan ook noodzakelijk zijn om de geheimhoudingsplicht te doorbreken of om persoonsgegevens te gebruiken voor een ander doel dan waarvoor deze initieel gebruikt zijn. Wanneer dit het geval is vormt deze toestemming geen grondslag voor de verwerking van persoonsgegevens. De toestemming geldt dan enkel om het verwerkingsverbod te doorbreken. Een aanvullende rechtmatige grondslag is dan noodzakelijk voor de daadwerkelijke verwerking.

9. Wijze van verwerking

Het uitgangspunt is dat persoonsgegevens zoveel mogelijk bij de betrokkene zelf worden verzameld. De wet gaat uit van subsidiariteit. Dit betekent dat verwerking alleen is toegestaan wanneer het doel niet op een andere manier kan worden bereikt. In de wet wordt ook gesproken over proportionaliteit. Dit betekent dat persoonsgegevens alleen worden verwerkt als dit in verhouding staat tot het doel. Wanneer met geen, of minder (belastende), persoonsgegevens hetzelfde doel bereikt kan worden moet daar altijd voor gekozen worden.

Persoonsgegevens moeten juist, ter zake dienend, up-to-date en niet bovenmatig veel zijn in het licht van het doel. Dit betekent dat alleen die persoonsgegevens mogen worden gebruikt die strikt noodzakelijk zijn voor het doel van de verwerking. Wanneer het bijvoorbeeld voldoende is om iemands contactgegevens te gebruiken is het niet nodig om ook een pasfoto en BSN te vragen. Voor het gebruik van het BSN gelden strenge regels. Wanneer ook met anonieme gegevens volstaan kan worden, mogen geen herleidbare persoonsgegevens gebruikt worden.

9.1 Organisatorische maatregelen

De gemeente zorgt er voor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden. Deze gegevens worden alleen verwerkt door medewerkers met een geheimhoudingsplicht. Ook is het van belang dat de medewerkers weten wat hun verantwoordelijkheid is. En hoe ze zorgvuldig om moeten gaan met persoonsgegevens. Het is dus belangrijk dat de medewerkers van de gemeente zich bewust zijn van de regels en gedragsnormen rondom privacy. Deze organisatorische maatregelen dragen ook bij aan de bewustwording binnen de gemeente. Denk hierbij aan het ontwikkelen van specifieke privacy protocollen en afwegingskaders. Maar ook in de vorm van het ondersteunen van de medewerkers door privacy trainingen en kennissessies. Medewerkers moeten persoonsgegevens verwerken zoals is bepaald in het algemeen privacybeleid, dit algemeen privacyreglement en de bijbehorende privacyregelingen.

9.2 Beveiliging

Door het beveiligen van persoonsgegeven moet de gemeente voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. Als uitgangspunt geldt dat naarmate de risico's van de verwerking hoger liggen er betere beveiligingsmaatregelen moeten worden getroffen. De gemeente heeft hiervoor een specifiek beleid opgesteld in de vorm van het Informatiebeveiligingsbeleid. Het is aan de gemeente om te bepalen hoe de persoonsgegevens organisatorisch en technisch worden beveiligd. Hoe de gemeente dit doet staat in het informatiebeveiligingsbeleid en in een eventueel aanvullend beveiligingsplan specifiek opgesteld voor een proces of registratie.

In ieder geval wordt de toegang en het gebruik van de systemen ten behoeve van de BRP en Suwinet gelogd. Middels steekproeven wordt gecontroleerd of het gebruik van de systemen en de verwerking van persoonsgegevens in lijn is met de wet- en regelgeving, het privacybeleid en dit algemeen privacyreglement. Ook voor overige systemen wordt gebruik gemaakt van logging. Als daar aanleiding toe is zal ook hier worden gecontroleerd of de systemen correct worden gebruikt.

9.3 Toegang tot persoonsgegevens

Uitsluitend de beheerder en de op grond van het autorisatieprotocol aangewezen gebruikers hebben rechtstreekse toegang tot persoonsgegevens. Wel voor zover dat voor de vervulling van hun functie of taak noodzakelijk is. Zij handelen in opdracht van de verwerkingsverantwoordelijke. Bij toekenning van autorisaties aan gebruikers wordt het geldende autorisatieprotocol gevolgd. Hierin is voor iedere applicatie, functie en rol vastgelegd welke autorisaties daaraan verbonden zijn.

9.4 Geheimhoudingsplicht

Voor ambtelijk medewerkers geldt dat zij in hun functie gehouden zijn tot geheimhouding van persoonsgegevens. Zij ondertekenen bij indienstneming een integriteitsverklaring. De personen voor wie niet al vanuit de ambt, het beroep of wettelijk voorschrift een geheimhoudingsplicht geldt zijn verplicht tot geheimhouding van de persoonsgegevens. Tenzij dit volgens een wettelijk voorschrift verplicht is om mededeling te doen aan derden. Zij ondertekenen een geheimhoudingsverklaring en committeren zich aan de gedragscode 'kleur bekennen'. Er wordt alleen autorisatie toegekend aan personen voor wie een verklaring omtrent gedrag is verkregen. Doorbreking van deze

geheimhoudingsplicht is enkel mogelijk wanneer de betrokkene hiervoor uitdrukkelijke en schriftelijk vastgelegde toestemming heeft verleend of via een wettelijk voorschrift.

9.5 Voorafgaande raadpleging

De Autoriteit Persoonsgegevens (AP) wordt geraadpleegd als uit een Data Protection Impact Assessment (DPIA) blijkt dat na het nemen van maatregelen de verwerking van persoonsgegevens een hoog risico zal opleveren. De gegevensverwerking mag nog niet starten totdat het onderzoek door de AP is afgerond of bericht is ontvangen dat er geen verder onderzoek wordt ingesteld. Een voorafgaande raadpleging is in ieder geval verplicht, als:

- a. Een BSN wordt verwerkt voor een ander doel dan waarvoor het BSN specifiek is bedoeld of;
- b. Een onderzoek plaatsvindt naar bijvoorbeeld een inwoner zonder dat deze inwoner wordt ingelicht
- c. (denk aan internetonderzoek of verborgen camera's); of
- d. Kennis over onrechtmatig of strafrechtelijk gedrag van een inwoner wordt gedeeld

10. Doorgifte aan derde landen

Persoonsgegevens mogen in principe niet worden doorgegeven naar een organisatie in een land buiten de EU. Onder doorgifte wordt bijvoorbeeld verstaan: het opslaan (bijvoorbeeld in de Cloud) of het doorsturen aan een organisatie buiten de EU. Hieronder valt niet het via internet zichtbaar maken van persoonsgegevens. De gemeente kan alleen persoonsgegevens doorgeven aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie wanneer voor dat land een adequaatheidsbesluit is afgegeven of op grond van door de Europese Commissie goedgekeurde afspraken. De gemeente besluit per situatie om persoonsgegevens door te geven aan derde landen.

11. Transparantie en communicatie

Informatieplicht

Betrokkenen worden in principe geïnformeerd over de verwerking. Het moment en de manier van informeren is afhankelijk hoe de persoonsgegevens worden verzameld. In bepaalde gevallen verwerkt de gemeente persoonsgegevens op basis van een wettelijke verplichting waarbij deze informatieplicht niet geldt.

Als de persoonsgegevens door de inwoner of medewerker zelf worden aangeleverd, dan moet deze over de verwerking van de gegevens vooraf worden geïnformeerd. Deze informatie bestaat uit:

- de identiteit van de gemeente en de identiteit van de Functionaris voor de Gegevensbescherming (FG);
- het doel van de verwerking waarvoor de gegevens zijn bestemd;
- de grondslag voor de verwerking;
- of en zo ja, met wie gegevens worden uitgewisseld;
- of gegevens worden verstrekt aan het buitenland;
- hoe lang de gegevens bewaard worden;
- de rechten die de betrokkenen heeft (inzage, correctie, verwijdering, beperking, bezwaar);
- het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens;
- het bestaan van geautomatiseerde besluitvorming of profilering (en de logica daarachter)

Als persoonsgegevens over de betrokkene niet direct bij deze persoon worden verkregen dan hoeft de betrokkene pas op een later moment geïnformeerd te worden. De betrokkene moet geïnformeerd worden voordat die persoonsgegevens door de gemeente worden vastgelegd of verder verwerkt worden. De betrokkene moet binnen een redelijke termijn en in ieder geval binnen een maand na verkrijging van de persoonsgegevens geïnformeerd worden op de bovenstaande punten.

12 Rechten van de betrokkene

12.1 Algemene uitgangspunten

Betrokkenen hebben bepaalde rechten zoals geformuleerd in deze paragraaf. Aan het uitoefenen van die rechten zijn voor de betrokkene geen kosten verbonden, tenzij dat bij wet is toegestaan. Betrokkenen kunnen zich bij het uitoefenen van die rechten laten bijstaan. De verwerkingsverantwoordelijke wijst betrokkenen op de mogelijkheden van rechtsbescherming en toezicht en op de rol daarin van de AP. Voor het uitoefenen van deze rechten dient de betrokkene een schriftelijk verzoek in bij de FG. Dit verzoek kan zowel op papier als per e-mail. De verwerkingsverantwoordelijke reageert zonder onnodige vertraging en in principe uiterlijk binnen een maand op het verzoek gerekend vanaf het moment van ontvangst daarvan. Er is de mogelijkheid om de termijn te verlengen met uiterlijk twee maanden. De verzoeker heeft recht op een afschrift van de gegevens die over diegene zijn vastgelegd. De verzoeker hoeft hiervoor niet te betalen. Indien een gewichtig belang van de verzoeker dit eist, kan aan het verzoek in een andere dan schriftelijke vorm worden voldaan. De verwerkingsverantwoordelijke draagt zorg voor de vaststelling van de identiteit van de verzoeker. De verwerkingsverantwoordelijke kan weigeren aan een verzoek te voldoen als dit noodzakelijk is in verband met:

- a. Het onderzoek, de opsporing en vervolging van strafbare feiten;
- b. de landsverdediging, nationale of openbare veiligheid;
- c. de bescherming van de onafhankelijkheid van de rechterlijke macht
- d. een taak op het gebied van toezicht, inspectie of regelgeving
- e. een algemeen belang van de Unie of de lidstaat
- f. gewichtige belangen van anderen dan de verzoeker, waaronder belangen van de verwerkingsverantwoordelijke.

Wanneer de verwerkingsverantwoordelijke een verzoek afwijst, is deze afwijzing deugdelijk gemotiveerd.

12.2 Recht op informatie

De verwerkingsverantwoordelijke informeert betrokkene tijdig en volledig over de persoonsgegevens die verwerkt worden. Het gaat hier om de doelen en de manieren waarop persoonsgegevens worden verwerkt, over de regels die daarvoor gelden, over de rechten die betrokkene heeft en hoe diegene die kan uitoefenen. Daarbij wordt betrokkene ook geïnformeerd over de plaats waar de documenten kunnen worden ingezien dan wel opgevraagd.

12.3 Recht op inzage

Iedereen kan bij de verwerkingsverantwoordelijke een verzoek indienen tot inzage van zijn of haar persoonsgegevens bij de gemeente 's-Hertogenbosch. De verwerkingsverantwoordelijke deelt een ieder op verzoek schriftelijk mee of persoonsgegevens over hen worden verwerkt. Als dat het geval is dan wordt aan de verzoeker desgewenst schriftelijk een volledig overzicht daarvan met informatie over het doel of de doelen van de gegevensverwerking, de grondslagen voor de verwerking, de gegevens of categorieën van gegevens waarop de verwerking betrekking heeft, de ontvangers of categorieën van ontvangers van de gegevens evenals de herkomst van de gegevens verstrekt. Indien de verzoeker dat wenst, verstrekt de verwerkingsverantwoordelijke tevens informatie over de systematiek van de geautomatiseerde gegevensverwerking.

12.4 Recht op correctie: verbetering, aanvulling, verwijdering en/of afscherming

Op schriftelijk verzoek van een betrokkene gaat de verwerkingsverantwoordelijke over tot verbetering, aanvulling, verwijdering en/of afscherming van de met betrekking tot de verzoeker verwerkte persoonsgegevens. Het gaat hierbij voor zover deze gegevens feitelijk onjuist, voor het doel van de verwerking onvolledig, niet ter zake dienend of bovenmatig zijn, dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek bevat de aan te brengen wijzigingen.

De verwerkingsverantwoordelijke deelt de verzoeker mee of aan het verzoek wordt voldaan. Als er niet of niet geheel wordt voldaan, wordt dat voldoende beredeneerd. De verwerkingsverantwoordelijke draagt er zorg voor dat een beslissing tot verbetering, aanvulling, verwijdering en/of afscherming zo spoedig mogelijk wordt uitgevoerd. De verwerkingsverantwoordelijke informeert derden daarover en verzekert zich ervan dat die derden hun bestanden aanpassen. De verwerkingsverantwoordelijke deelt de verzoeker mee aan welke derden die informatie is verstrekt.

12.5 Recht op beperking van de verwerking

Indien de betrokkene de juistheid, rechtmatigheid of noodzaak van de persoonsgegevens betwist, kan de betrokkene bij de verwerkingsverantwoordelijke verzoeken om een beperking van de verwerking. De verwerking wordt in dat geval beperkt tot de opslag van de gegevens, totdat de juistheid, rechtmatigheid of de noodzaak is vastgesteld. De verwerkingsverantwoordelijke beoordeelt of de

beperking gerechtvaardigd is. De beheerder beëindigt de verwerking zo spoedig mogelijk, als de verwerkingsverantwoordelijke het bezwaar gerechtvaardigd acht.

12.6 Recht van bezwaar

Indien de rechtmatige grondslag voor een bepaalde verwerking is gelegen in een taak van algemeen belang, de uitoefening van openbaar gezag of het gerechtvaardigde belang van de verwerkingsverantwoordelijke, kan de betrokkene bij de FG te allen tijde bezwaar aantekenen tegen die verwerking in verband met zijn bijzondere persoonlijke omstandigheden. De verwerkingsverantwoordelijke beoordeelt of het bezwaar gerechtvaardigd is. De verwerkingsverantwoordelijke beëindigt de verwerking zo spoedig mogelijk, indien de verwerkingsverantwoordelijke het bezwaar gerechtvaardigd acht. Verzet tegen de verwerking voor commerciële of charitatieve doelen is altijd gerechtvaardigd.

12.7 Recht op dataportabiliteit

Dataportabiliteit is het recht van de betrokkene om persoonsgegevens overgedragen te krijgen in een gangbaar en door de computer leesbare vorm. Het recht op dataportabiliteit is niet van toepassing op gegevens die gebruikt zijn voor de uitvoering van gemeentelijke taken.

12.8 Geautomatiseerde besluitvorming en profilering

De betrokkene heeft het recht om niet te worden onderworpen aan een volledig geautomatiseerde beslissing, die serieuze impact heeft op diegene. Dit betekent dat we bijvoorbeeld niet automatisch een besluit kunnen genereren over een door de inwoner ingediende aanvraag. Hier moet altijd een medewerker naar kijken. Wanneer we wel automatisch een beslissing genereren moeten we de inwoner daar vooraf over inlichten. Ook zijn we verplicht om de aanvraag door een persoon te laten beoordelen. Betrokkene heeft het recht om bezwaar te maken tegen een dergelijke verwerking bij de FG en te verlangen van de gemeente dat wij inzichtelijk maken hoe we tot de beslissing zijn gekomen.

12.9 Rechtsbescherming

Een beslissing van de verwerkingsverantwoordelijke op een verzoek van de betrokkene is een besluit in de zin van de Algemene wet bestuursrecht waartegen bezwaar en beroep openstaan.

12.10 Klachtenprocedure

Elke betrokkene heeft het recht bij de verwerkingsverantwoordelijke een klacht in te dienen:

- a. tegen een beslissing op een verzoek als bedoeld in de artikelen 20 t/m 25;
- b. tegen een beslissing naar aanleiding van de aantekening van verzet als bedoeld in artikel 18;
- c. tegen de wijze waarop de verwerkingsverantwoordelijke, beheerder of verwerker de regels uit dit reglement uitvoert.

De verwerkingsverantwoordelijke reageert zo spoedig mogelijk, maar uiterlijk binnen zes weken na ontvangst, schriftelijk en met redenen omkleed op de klacht. Betrokkene kan zich bij de indiening en behandeling van zijn klacht laten bijstaan. De verwerkingsverantwoordelijke kan het advies van de AP inwinnen. De verwerkingsverantwoordelijke kan tot het oordeel komen dat de klacht onterecht is dan wel geheel of gedeeltelijk terecht.

Indien de verwerkingsverantwoordelijke de klacht niet of slechts gedeeltelijk honoreert, kan de betrokkene een klacht indienen bij de AP. De verwerkingsverantwoordelijke informeert de betrokkene over die mogelijkheid en geeft de contactgegevens door. Indien de verwerkingsverantwoordelijke oordeelt dat de klacht geheel of gedeeltelijk terecht is, wordt beslist om:

- a. het verzoek van betrokkene alsnog geheel of gedeeltelijk te honoreren;
- b. het verzet van betrokkene alsnog te honoreren;
- c. alsnog uitvoering te geven aan de in het reglement opgenomen regels, wat kan inhouden een handelen of een nalaten, waaronder begrepen een herstellen of een stoppen;
- d. de schade die betrokkene heeft geleden, waaronder eventuele immateriële schade, te vergoeden.

Indien de betrokkene van mening is dat de verwerkingsverantwoordelijke zijn plichten of verantwoordelijkheden op grond van de AVG niet, niet tijdig of niet behoorlijk nakomt, dan wel wanneer de betrokkene de uitleg die de verwerkingsverantwoordelijke geeft aan de wet- en regelgeving betwist, kan betrokkene een klacht indienen bij de AP.

12.11 Audio en video-opnamen

Als een inwoner een geluidsopname van een gesprek met een gemeentelijk medewerker wil maken dan mag dat. De inwoner moet daarvoor wel zelf actief deelnemen aan het bewuste gesprek, of handelen in opdracht van een deelnemer. Het opnemen van een gesprek moet vooraf aan worden gegeven. Ook een medewerker van de Gemeente 's-Hertogenbosch mag besluiten om een geluidsopname te maken. We maken hierbij gebruik van de spelregels die zijn opgesteld door de Nationale Ombudsman. De onderstaande spelregels gelden bij het maken van audio-opnamen:

- a. De gesprekspartner verstrekt aan de Gemeente 's-Hertogenbosch (en andere gesprekspartners) een kopie van de gemaakte geluidsopname als deze dat wenst of andersom als de gemeente de opname maakt;
- b. Een geluidsopname mag op geen enkele wijze worden bewerkt, tenzij dit wordt meegedeeld en met instemming;
- c. De geluidsopname is alleen bedoeld voor het terugluisteren van het gesprek in de huiselijke kring. De geluidsopname mag dus niet, geheel of gedeeltelijk, gepubliceerd of anderszins openbaar gemaakt worden (delen met anderen, online via social media en dergelijke). Dit mag alleen met toestemming van de andere gesprekspartij(en);
- d. Het maken van beeldopnames van een gesprek is niet toegestaan;
- e. Indien een gesprek bij een inwoner thuis plaatsvindt in een ruimte waar een camera (met of zonder geluid) aanwezig is, wordt dit voor de start van het gesprek verteld aan de medewerker. De medewerker kan er dan voor kiezen om het gesprek op een andere locatie plaats te laten vinden;
- f. Alleen als er zwaarwegende redenen zijn kan de gemeente het maken van een geluidsopname niet toestaan. In dat geval legt de medewerker van de Gemeente 's-Hertogenbosch uit wat die zwaarwegende redenen zijn. Wel zal een alternatief aangeboden worden dat kan bestaan uit:
 - het bieden van de mogelijkheid om een gemachtigde of derde mee te nemen naar het gesprek;
 - het opnemen door de Gemeente 's-Hertogenbosch dat afgeluisterd mag worden indien wenselijk;
 - het aanbieden van een globale schriftelijke weergave van het gesprek.

13. Plichten van de gemeente

13.1 Register van verwerkingen

Met ingang van 25 mei 2018 heeft de gemeente er extra verplichtingen bij gekregen. De gemeente is verplicht om te documenteren welke persoonsgegevens worden verwerkt, wat het doel ervan is, van wie of waar deze gegevens afkomstig zijn en met wie deze gegevens worden gedeeld. Daarnaast moeten we per verwerking documenteren en verantwoorden op basis van welke wettelijke grondslag de gemeente deze persoonsgegevens verwerkt.

13.2 Bewaartermijnen

De gemeente bewaart de persoonsgegevens niet langer dan nodig is voor het uitvoeren van gemeentelijke taken, of zoals vastgelegd in de Archiefwet. In de AVG of UAVG worden geen bewaartermijnen genoemd. De hoofdregel is: bewaren mag zolang het noodzakelijk is voor het doel van de verwerking. In een aantal wetten zijn specifieke bewaartermijnen opgenomen voor bepaalde persoonsgegevens. Als geen bewaartermijn aanwezig is dan moet goed kunnen worden onderbouwd waarom persoonsgegevens voor een bepaalde termijn worden bewaard. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel worden deze zo snel mogelijk verwijderd.

13.3 Vernietiging

Na afloop van de bewaartermijnen moeten de persoonsgegevens worden vernietigd of geanonimiseerd. Dit geldt niet alleen voor de gegevens zelf, maar ook voor kopieën en back-ups. Voor alle persoonsgegevens geldt dat de vernietiging onomkeerbaar moet zijn. Het gaat dus niet om het plaatsen van de bestanden in de prullenbak en de prullenbak legen, maar bijvoorbeeld om het overschrijven van data met nullen, enen en willekeurige karakters (data wiping). De gemeente draagt zorg voor tijdige verwijdering en vernietiging van de verwerkte en opgeslagen gegevens. Daartoe worden in opdracht van de afdeling jaarlijks schonings-, en vernietigingslijsten opgesteld.

13.4 Meldplicht datalekken

De meldplicht datalekken houdt in dat de gemeente zo snel mogelijk (binnen 72 uur) een melding doet bij de AP zodra een ernstig datalek zich heeft voorgedaan. Een datalek is een inbreuk op de beveiliging die grote nadelige gevolgen heeft voor de inwoner of voor de bescherming van de persoonsgegevens. Denk hierbij aan een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak op het netwerk. In geval van signalering van een datalek wordt de gemeentelijke procedure gevolgd. Medewerkers, verwerkers en derden zullen de inbreuk melden bij de FG. Indien een inbreuk waarschijnlijk ernstige nadelige gevolgen zal hebben voor de bescherming van persoonsgegevens wordt hiervan melding gedaan bij de AP. Wanneer een inbreuk waarschijnlijk ernstige nadelige gevolgen zal hebben voor de betrokkene, wordt ook de betrokkene in kennis gesteld. Alle datalekken worden gedocumenteerd. Op basis hier van kan de AP controleren of wij aan de meldplicht voldoen.

13.5 Verwerkersovereenkomsten

Verwerkersovereenkomsten worden afgesloten wanneer andere partijen – ook wel verwerkers genoemd – in opdracht van de gemeente persoonsgegevens verwerken. Denk aan een schuldhulpverlening instantie die van de gemeente de opdracht krijgt de schuldenproblematiek aan te pakken. Hiervoor krijgt de instantie toegang tot de gemeentelijke gegevens. Uiteraard moeten er duidelijke afspraken worden gemaakt. Denk hierbij aan welke gegevens men nodig heeft om haar taak uit te oefenen. Ook de manier waarop de organisatie de gegevens heeft beveiligd en wat zij moet doen bij een datalek. De gemeente heeft een standaard verwerkersovereenkomst die in al deze gevallen wordt gebruikt.

13.6 Bewustwording en training

De verwerkingsverantwoordelijke draagt zorg voor een regelmatige bewustwording van alle medewerkers. Dit om te verzekeren dat ze de processen van persoonsgegevensverwerking, de daarvoor geldende regels, de gedragscode en hun eigen rol daarin begrijpen en toe kunnen passen. De gemeente kan deelname aan deze scholing verplicht stellen.

13.7 Het Data Protection Impact Assessment (DPIA)

Met een DPIA worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt. De gemeente 's-Hertogenbosch voert deze alleen uit wanneer:

- er een (geautomatiseerde) verwerking plaatsvindt met een hoog risico,
- er een (geautomatiseerde) verwerking plaatsvindt waarvan de Autoriteit Persoonsgegevens heeft aangegeven dat daarvoor een DPIA verplicht is;
- er een grootschalige verwerking plaatsvindt;
- of wanneer er een grootschalige monitoring van openbare ruimten plaatsvindt.

13.8 Data Protection by Design en Data Protection by Default

Bij de aanschaf of ontwikkeling van producten, diensten, systemen of processen moet in de ontwerpfase en gedurende de gehele verdere levensduur van een product, dienst, systeem of proces, altijd rekening worden gehouden met de bescherming van persoonsgegevens (privacy by design). Dit gebeurt onder andere door systemen en processen zo in te richten dat standaard alleen die gegevens worden verwerkt die nodig zijn (privacy by default). Als blijkt dat bij een proces of systeem gevoelige of bijzondere persoonsgegevens worden verwerkt en dit mogelijk een hoog privacyrisico met zich meebrengt dan zijn we verplicht om een DPIA uit te voeren.

13.9 Functionaris voor de gegevensbescherming

De gemeente heeft een functionaris voor de gegevensbescherming (FG) aangesteld. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de FG zijn informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van de AP. De FG heeft een belangrijke coördinerende rol en adviseert over oplossingen ten aanzien van privacy en gegevensverwerking. De FG houdt vanuit een onafhankelijke positie intern toezicht op de manier waarop door de gemeente wordt omgegaan met persoonsgegevens. Belangrijk is ook dat de FG aan de voorkant een rol speelt bij de inrichting van processen. En als laatste is de FG het formele aanspreekpunt is voor inwoners als zij hun rechten als betrokkene willen uitoefenen. De bevoegdheden van de FG zijn opgenomen in het 'Reglement voor de Functionaris voor de Gegevensbescherming', zoals vastgesteld door het College van B&W. Het is niet de bedoeling dat de FG de taken op het gebied van bescherming van de privacy van de afdelingen overneemt. De afdelingen

hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens. Voor vragen over privacy of deze toelichting kunt u contact opnemen met de FG via: privacy@s-hertogenbosch.nl

14 Verantwoordelijkheid

De sector, respectievelijk afdeling, is verantwoordelijk voor de wijze waarop zij persoonsgegevens verwerkt. De afdelingshoofden binnen de Gemeente 's-Hertogenbosch zien er op toe dat al wat in dit reglement is vastgelegd op een juiste en zorgvuldige wijze wordt uitgevoerd door de medewerkers die onder hun leiding en toezicht werken. Zij dragen er zorg voor dat de medewerkers op de hoogte zijn van de inhoud van het privacybeleid en de inhoud van dit reglement, evenals zich committeren aan en gedragen. Aan de medewerkers die vanuit hun functie persoonsgegevens inzien en verwerken worden autorisatierechten toegekend namens de beheerder conform het geldende autorisatieprotocol.

De FG of de medewerkers belast met privacy, zoals de Privacy Officer of Sectoraal Privacy Coördinator, kunnen adviseren ten aanzien van dan wel oordelen of een bepaalde gegevensverwerking conform het beleid en het reglement wordt uitgevoerd. Van operationele adviezen en oordelen van de Privacy Officer of Sectoraal Privacy Coördinator kan gemotiveerd worden afgeweken. Adviezen van de FG dienen altijd te worden opgevolgd. Als de aanwijzing(en) van de FG niet binnen een redelijke termijn wordt opgevolgd, wordt het volgende escalatiemodel gehanteerd:

1. De leidinggevende van de desbetreffende sector of afdeling wordt geïnformeerd en draagt verantwoordelijkheid voor de opvolging; Bij het niet opvolgen van de aanwijzing wordt:
2. De directeur van de desbetreffende sector wordt geïnformeerd en draagt verantwoordelijkheid voor de opvolging; Bij het niet opvolgen van de aanwijzing wordt:
3. De directeur Middelen & Dienstverlening wordt geïnformeerd en draagt verantwoordelijkheid voor de opvolging; Bij het niet opvolgen van de aanwijzing wordt: Het College geïnformeerd.

15 De 10 Gouden regels van privacy & informatiebeveiliging

Om als gemeente 's-Hertogenbosch voor iedereen op een duidelijke en begrijpelijke wijze het belang van het zorgvuldig omgaan met persoonsgegevens, zijn er 10 regels opgesteld. Deze bestaan uit 6 regels die specifiek zien op het werken met (en verwerken van) persoonsgegevens. De andere 4 regels zijn de zien op de informatiebeveiliging, maar zijn ook van toepassing op het zorgvuldig omgaan met persoonsgegevens. Deze 10 regels worden gezamenlijk aangeduid als de 10 gouden regels van privacy & informatiebeveiliging. Iedere sector, afdeling en medewerker dient deze gouden regels te kennen, te respecteren en toe te passen in de dagelijkse werkzaamheden. Per sector of per afdeling is het mogelijk om binnen deze vaststaande 10 regels en de kaders een nadere invulling en toelichting te geven.

De 10 gouden regels zijn:

1. Behandel persoonsgegevens vertrouwelijk en integer
2. Verwerk niet meer persoonsgegevens dan nodig
3. Motiveer en leg vast wat je doet
4. Leg uit waarom we persoonsgegevens verwerken en wees transparant
5. Weet wanneer je persoonsgegevens mag delen met anderen
6. Ga zorgvuldig met persoonsgegevens om
7. Ga verantwoord om met wachtwoorden
8. Ken de risico's van e-mail, internet en sociale media
9. Ga verantwoord om met mobiele faciliteiten
10. Maak melding van beveiligingsincidenten

16. Wijziging en aanvullingen

Wijzigingen van of aanvullingen op het Algemeen Privacybeleid Gemeente 's-Hertogenbosch en/of het Algemeen Privacyreglement Gemeente 's-Hertogenbosch worden ter goedkeuring en vaststelling voorgelegd aan het College van Burgemeester en Wethouders.

De verschillende sectoren van de Gemeente 's-Hertogenbosch (w.o. WXL) kunnen aanvullende reglementen of overige regelingen dan wel uitvoeringsregels opstellen, waarmee invulling wordt gegeven aan het algemeen beleid en de kaders zoals vastgelegd in het Algemeen Privacybeleid en/of het Algemeen Privacyreglement van de Gemeente 's-Hertogenbosch. De goedkeuring en vaststelling van sectorale aanvullingen op het Algemeen Privacybeleid en/of het Algemeen Privacyreglement van de Gemeente 's-Hertogenbosch geschiedt door het Algemeen Management Team.

17. Inwerkingtreding en citeertitel

Dit reglement wordt aangehaald als Algemeen Privacyreglement Gemeente 's-Hertogenbosch en treedt in werking na vaststelling door het College van Burgemeester en Wethouder.

*De waarnemend secretaris,
mr. drs. J.W. Hansum MBA MCM
De Burgemeester,
drs. J.M.L.N. Mikkers*