gemeente Baarn

GEMEENTEBLAD

Officiële uitgave van de gemeente Baarn

Nr. 104960

18 mei

2018

Gemeente Baarn - Privacybeleid gemeente Baarn 2018

Collegebesluit
Collegenummer: 47990
Openbaar

Onderwerp: Privacybeleid gemeente Baarn 2018

Burgemeester en wethouders van de gemeente Baarn
b e s l u i t e n:

1. Het privacybeleid gemeente Baarn 2018 vast te stellen
2. Indien het verwerkingenregister gereed is een openbare versie te publiceren

Baarn, 15 mei 2018
burgemeester en wethouders van Baarn,
secretaris burgemeester

Privacybeleid - Gemeente Baarn 2018

Inhoudsopgave

1. Inleiding
De gemeente Baarn verzamelt en gebruikt persoonsgegevens voor de dienstverlening aan inwoners en bedrijven en voor haar eigen bedrijfsorganisatie. Persoonsgegevens zijn gegevens die direct of indirect informatie verschaffen over een natuurlijk persoon. De gemeente is verantwoordelijk voor de bescherming van deze persoonsgegevens.
Voorbeelden van dienstverlening/processen waarbij de gemeente persoonsgegevens gebruikt zijn:
- gemeentelijke basisregistratie;
- registratie van gegevens voor vergunningaanvragen;
- registratie van gegevens voor de inning en heffing van belastingen;
- registratie van gegevens voor jeugdhulp en WMO-voorzieningen;
- registratie van gegevens voor bezwaar en beroep en klachten;
- personeelsadministratie.

De bescherming van persoonsgegevens speelt een steeds belangrijkere rol door de:
• technologie die zich steeds sneller ontwikkelt,
• toename in dataverkeer,
• toename in het verzamelen en delen van gegevens met ketenpartners,
• risico's van cybercrime,
• samenleving die steeds kritischer wordt,
• behoefte en rechten van inwoners om inzicht in het gebruik van zijn of haar persoonsgegevens,
• toename van de hoeveelheid gevoelige informatie van personen door de decentralisaties in het sociaal domein.

Het gebruik van persoonsgegevens raakt het privéleven van inwoners. Daarom is het gebruik van persoonsgegevens aan regels gebonden. Voor de gemeente Baarn zijn deze regels leidend. Dit privacybeleid geeft de kaders en uitgangspunten voor een zorgvuldig, juist en veilig gebruik van persoonsgegevens binnen de geldende regelgeving. Het beleid geldt voor een ieder die namens de gemeente gebruik maakt van persoonsgegevens. Inwoners moeten erop kunnen vertrouwen dat hun persoonsgegevens in goede handen zijn bij de gemeente Baarn.

2 Reikwijdte privacybeleid
Het privacybeleid is van toepassing op de hele organisatie en alle processen waarbij persoonsgegevens worden gebruikt. Ook de processen van de raad en die van bestuurlijke (advies)commissies waarbij persoonsgegevens worden gebruikt vallen onder de reikwijdte van dit beleid.

Wat onder persoonsgegevens wordt verstaan, om wiens persoonsgegevens het gaat, hoe de gemeente er aan komt en wanneer de gemeente persoonsgegevens mag gebruiken wordt hieronder beschreven.

Het beleid geldt voor een ieder die namens de gemeente Baarn gebruik maakt van persoonsgegevens.

Onder gebruik wordt verstaan: verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, aan derden geven, verspreiden of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, en het afschermen, uitwissen of vernietigen van gegevens.

Het privacybeleid geldt als algemeen beleid. Hierin zijn de kaders, uitgangspunten, taken en verantwoordelijkheden en maatregelen beschreven om de persoonsgegevens te beschermen. Voor bepaalde domeinen kan het nodig zijn om aanvullend een specifiek privacybeleid vast te stellen.

2.1 Wat is een persoonsgegeven en hoe komen we eraan?
Het gaat om gegevens die direct of indirect informatie verschaffen over een natuurlijk persoon. Naam, geboortedatum, geslacht en adresgegevens zijn directe gegevens. Uiterlijke, sociale en economische kenmerken is indirecte informatie die in combinatie met andere gegevens kan leiden tot identificatie van een persoon.

De wet maakt onderscheid tussen gewone persoonsgegevens en bijzondere persoonsgegevens. Bijzondere persoonsgegevens zijn gegevens die gevoelige informatie over een persoon verschaffen, zoals gegevens over gezondheid of strafrechtelijke gegevens. Het gebruik van bijzondere persoonsgegevens is verboden, tenzij in de wet een uitzondering op dit verbod is opgenomen.

Persoonsgegevens worden zoveel mogelijk door de persoon zelf verstrekt. Soms zijn gegevens afkomstig van derden, zoals uitkeringsinstanties.

2.2 Van wie worden persoonsgegevens gebruikt, wanneer en waarom?

Van iedereen die gebruik maakt van de dienstverlening van de gemeente Baarn. En iedereen die werkzaam is voor de gemeente Baarn.

Binnen de gemeente Baarn gebruiken we persoonsgegevens alleen voor een bepaald doel. Het doel van het gebruik en de soort gegevens kunnen per product of dienst verschillen. Het doel kan zijn het afhandelen van aanvragen, heffen en innen van belastingen, verstrekken van uitkeringen of subsidies of betalen van huur voor een stukje grond.

Binnen de gemeente Baarn verzamelen en gebruiken we verschillende soorten gegevens. Dit kunnen naam en adresgegevens zijn, maar soms ook gevoelige gegevens zoals het BSN nummer of gezondheidsgegevens.

Persoonsgegevens mogen alleen worden gebruikt als daar een wettelijke basis voor is. Deze basis kan slechts zijn: uitvoeren van een overeenkomst, uitvoeren van een wettelijke verplichting, uitvoeren van een publieke taak, bij een vitaal belang, een gerechtvaardigd belang of met toestemming.

2.3 Verhouding tot Informatiebeveiliging(sbeleid) Privacy(beleid) richt zich op persoonsgegevens. Daarbij richt het zich met name op het passend gebruik. Als persoonsgegevens worden verzameld en gebruikt moeten deze worden voorzien van passende beveiliging. Het Informatiebeveiligingsbeleid voorziet in het implementeren van maatregelen die deze bescherming van privacy mogelijk maken. Door deze nauwe verwevenheid is een goede samenwerking tussen privacy en security (informatiebeveiliging) noodzakelijk.
3 *Wet- en regelgeving*
De eerbiediging van de persoonlijke levenssfeer (privacy) is een grondrecht en onder meer geregeld in:
- artikel 8 van het Europese verdrag voor de rechten van de mens (EVRM)
- artikelen 7 en 8 Handvesten Grondrechten EU;
- artikel 10 Grondwet;

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

Er zijn ook nog andere wetten die het gebruik van persoonsgegevens regelen en die, indien van toepassing, voorgaan op de Uitvoeringswet AVG, omdat zij specifieke regels bevatten op hun terrein. Te denken valt aan:
- de Wet basisregistratie personen (Wet BRP)
- de Wet politiegegevens;
- de Jeugdwet;
- de Wet maatschappelijke ondersteuning 2015.

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

4 Doel en uitgangspunten privacybeleid
4.1 Doelstelling
Doel van dit privacybeleid is het beschrijven van kaders en uitgangspunten voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacyrechten van personen waarvan de gemeente Baarn persoonsgegevens gebruikt. Het privacybeleid draagt bij aan:
· het beschermen van de privacy van personen van wie de gemeente gegevens gebruikt of laat gebruiken,
· maatschappelijk vertrouwen en draagvlak,
· naleving van de wet
· beheersen van gemeentelijke afbreuk- en aansprakelijkheidsrisico's,
· verantwoording af kunnen leggen aan de raad, waar nodig de Autoriteit Persoonsgegevens of de rechter,
· het in kunnen spelen op wettelijke en technologische ontwikkelingen.

4.2 Uitgangspunten
Iedereen werkzaam binnen de organisatie is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacyrechten van personen. Het gebruik van persoonsgegevens is rechtmatig, behoorlijk en transparant. De uitgangspunten hierbij zijn:
· Het gebruik is noodzakelijk, voor een bepaald doel en heeft een wettelijke basis. Deze basis kan slechts zijn: uitvoeren van een overeenkomst, uitvoeren van een wettelijke verplichting, uitvoeren van een publieke taak, bij een vitaal belang, een gerechtvaardigd belang of in het uiterste geval met toestemming.
· Alleen persoonsgegevens die noodzakelijk zijn voor het doel worden gebruikt;
· Persoonsgegevens zijn correct en actueel.
· Alleen die mensen die de gegevens nodig hebben voor de uitoefening van hun taak hebben toegang tot deze gegevens.
· Degene van wie de persoonsgegevens worden gebruikt is vooraf in eenvoudige en duidelijk taal geïnformeerd dat zijn/haar persoonsgegevens worden gebruikt en voor welk doel.
· Het gebruik van persoonsgegevens is inzichtelijk.
· Rechten van diegene van wie de persoonsgegevens worden gebruikt, zoals 'recht op inzage, correctie, verwijdering' worden opgevolgd, voor zover de wetgeving dit toelaat.
· Als het gebruik niet meer noodzakelijk is voor het doel, dan worden de persoonsgegevens verwijderd of geanonimiseerd.
· Persoonsgegevens zijn beveiligd door middel van technische en organisatorische maatregelen.
· Evenwichtige balans tussen bescherming persoonsgegevens, dienstverlening en werkbaarheid. Waar nodig en mogelijk wordt het advies en de deskundigheid van wetgever, toezichthouder of koepelorganisatie betrokken bij dilemma's.

5 *Organisatie van het privacy*
5.1 Doelstelling

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

5.2 Verantwoordelijkheden

College van burgemeester en wethouders

De rechtspersoon/overheidsinstantie die het doel en de middelen voor het gebruik van persoonsgegevens vaststelt is verwerkingsverantwoordelijke" in de zin van de Avg.
De gemeente kent verschillende bestuursorganen die zelf voor bepaalde processen zelf de doelen en middelen vaststellen. Omdat college van burgemeester en wethouders in het algemeen binnen de gemeente het orgaan is die doel en middelen vaststellen zijn zij bestuurlijk eindverantwoordelijk voor de bescherming van persoonsgegevens binnen de gemeente. Ook voor persoonsgegevens die door derden worden gebruikt is het college eindverantwoordelijk, als zij het doel en de middelen van het gebruik vaststellen. Het college stelt daarom het privacybeleid vast en mandateert de feitelijke verantwoordelijkheid aan de managers. Het college informeert de raad en legt verantwoording af aan de raad via de P&C cyclus.
Het management
De managers zijn feitelijk verantwoordelijk voor het juiste, zorgvuldige en veilige gebruik van persoonsgegevens, voor wat betreft de bij het team betrokken processen waarbij persoonsgegevens worden gebruikt. De teammanager is eindverantwoordelijk voor:
· de melding aan de Functionaris Gegevensbescherming (FG) van de bij zijn/haar programma betrokken processen waarbij persoonsgegevens worden gebruikt;
· afsluiten van verwerkersovereenkomsten als wordt ingekocht en het gebruik van persoonsgegevens onderdeel is van de geleverde dienstverlening;
· melding van beveiligingsincidenten/datalekken aan de Chief Information Security Officer (CISO)/Functionaris Gegevensbescherming (FG);
· sturen op privacybewustzijn en naleving van regels en richtlijnen (gedrag en risicobewustzijn).

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

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

5.3 Taken en rollen

Functionaris Gegevensbescherming (FG),
Het college heeft een functionaris gegevensbescherming in de zin van artikel 37 AVG benoemd. De taken van de FG zijn:
- toezicht houden op de naleving van de privacyvoorschriften, met inbegrip van de toewijzing van verantwoordelijkheden, bewustwording en opleiding;
- verzamelen van inventarisaties van gegevensverwerkingen;
- bijhouden van het interne meldingenregister;
- informeren en adviseren aan bestuur, management en medewerkers van de organisatie
- betrokken worden bij het opstellen van een gegevensbeschermingseffectbeoordeling (PIA);
- contactpersoon Autoriteit Persoonsgegevens.

Chief Information Security Officer (CISO),
De CISO houdt toezicht op de informatiebeveiliging en rapporteert hierover aan het management. Hij bewaakt de voortgang van aanbevelingen uit het Informatiebeveiligingssplan en adviseert over het te voeren beleid. De CISO bevordert concernbreed het beveiligingsbewustzijn.

Privacybeheerder/ Information Officer (ISO)
Voor de informatiebeveiliging zijn zogenaamde beveiligingsbeheerders aangesteld. Binnen de gemeenten Baarn fungeren de beveiligingsbeheerders tevens als vooruitgeschoven posten voor privacy. Ook anderen dan beveiligingsbeheerders kunnen zijn aangewezen als privacybeheerder. Zij zijn de contactpersoon voor de FG en fungeren als aanspreekpunt voor de bescherming van persoonsgegevens binnen het team.

6. Maatregelen

Met de maatregelen beschreven in dit hoofdstuk kunnen de privacyvoorschriften worden nageleefd en de risico's worden beperkt.

Het zijn wettelijke maatregelen om persoonsgegevens rechtmatig, behoorlijk en transparant te gebruiken. Door het treffen van deze maatregelen kan de gemeente Baarn voldoen aan haar verantwoordingsplicht.

6.1 Communicatie over de rechten van diegene wiens gegevens worden gebruikt.

Iedereen heeft recht op informatie over de persoonsgegevens die de gemeente van hem of haar gebruikt en over het doel waarvoor de gegevens worden gebruikt, om deze in te zien en ook om deze gegevens te verbeteren, aan te vullen te verwijderen of af te schermen als deze feitelijk onjuist, onvolledig of niet relevant zijn. De gemeente communiceert actief over deze rechten op de gemeentelijke website en in andere uitingen.

6.2 Register van verwerkingsactiviteiten
De gemeente houdt een register bij met alle processen waarbij persoonsgegevens worden gebruikt. Hierin worden onder andere het doel van het gebruik, de groep personen van wie de gegevens worden gebruikt, welke organisaties de gegevens ontvangen en bewaartermijnen opgenomen. Dit register is openbaar. Inwoners hebben hierdoor inzicht in de wijze waarop hun persoonsgegevens worden gebruikt.

6.3 Bewustwording
De mens is de zwakste schakel in de omgang met persoonsgegevens. Bewustwording is essentieel voor het borgen van privacy in de organisatie. Het is belangrijk dat iedereen die werkt met privacygevoelige informatie zich bewust is van het belang om hier zorgvuldig mee om te gaan. Doorlopend wordt er aandacht geschonken aan de bewustwording, door middel van trainingen, bijeenkomsten en aandacht in werkoverleg en evaluatie- en prestatiegesprekken.

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

6.5 Afsluiten van verwerkersovereenkomsten
De gemeente is eindverantwoordelijke als zij doel en middelen vaststelt van het gebruik van persoonsgegevens. Ook als gebruik wordt gemaakt van leveranciers. De leverancier is dan een verwerker en het is wettelijk verplicht met hem een verwerkersovereenkomst af te sluiten. Hierin worden onder andere afspraken gemaakt over beveiliging, doelen van gebruik, toezicht, locatie van data, datalekken, geheimhouding.

De gemeente gebruikt in beginsel het model verwerkersovereenkomst van de Informatiebeveiligingsdienst (IBD).

6.6. Melding b eveiligingsincidenten en datalekken
Als een inbreuk op de beveiliging zich voordoet worden maatregelen getroffen om de gevolgen van de inbreuk te beperken en om herhaling te voorkomen. Inbreuken op de beveiliging waardoor persoonsgegevens verloren gaan of waarvan onrechtmatig gebruik niet is uitgesloten zijn datalekken. Een datalek dat grote risico's heeft voor de bescherming van persoonsgegevens wordt door de Functionaris Gegevensbescherming gemeld bij de Autoriteit Persoonsgegevens. Als het datalek ongunstige gevolgen heeft voor de persoonlijke levenssfeer van degene van wie de persoonsgegevens zijn, wordt dit aan hem of haar gemeld.
De gemeente heeft een protocol meldplicht datalekken en houdt een register bij met datalekken.

6.7 Privacy-risico's van te voren in beeld brengen
Voor (veranderingen in) processen, diensten, producten en informatiesystemen, waar persoonsgegevens worden gebruikt, is het van belang van te voren goed te bedenken welke privacyaspecten een rol (kunnen) spelen, welke effect het gebruik heeft op de privacy en welke oplossingen ervoor zorgen dat privacyproblemen zich niet voordoen.

De gemeente doet dit door:
- Gegevensbeschermingseffectbeoordelingen (Privacy Impact analyses) uit te voeren
- Bij het ontwerp rekening te houden met privacy-aspecten en bij standaardinstellingen de privacy maximaal te waarborgen (Privacy by design of privacy by default).

Privacy impact analyses (PIA's)
Voor een proces/product/dienst/systeem waarbij persoonsgegevens worden gebruikt en waarbij hoge privacyrisico's spelen moet van te voren een PIA worden uitgevoerd. Een systematische beschrijving van het beoogde gebruik van persoonsgegevens, de doeleinden, de noodzaak en de proportionaliteit van het gebruik van persoonsgegevens, de risico's en (voorgenomen) maatregelen. Het doel is om de impact van het gebruik op de bescherming van persoonsgegevens in kaart te brengen.

Per PIA wordt advies aan de FG gevraagd.

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

Privacy by default betekent dat de standaard instellingen in systemen zo zijn ingesteld dat privacybescherming maximaal is geborgd.

Bij het toepassen van Privacy by design en – default wordt advies aan de FG gevraagd.

6.8 Toezicht
Om de bescherming van persoonsgegevens te waarborgen houdt de FG intern toezicht op de naleving van de privacyregelgeving. De FG beschikt daarbij over alle bevoegdheden die uit de wetgeving voortvloeien, zoals het doen van onderzoek, betreden van ruimtes, vragen van inlichtingen. De FG deelt zijn bevindingen met de verantwoordelijken en geeft zonodig aanbevelingen. De FG brengt jaarlijks verslag uit over de naleving van de privacyregelgeving aan het college van burgemeester en wethouders.

Inwerkingtreding
Dit privacybeleid treedt in werking één dag na bekendmaking.

Baarn, 15 mei 2018

Burgemeester en wethouders van Baarn,

Drs. A. Najib M.A. Röell
Gemeentesecretaris Burgemeester