



Privacybeleid en Privacyreglement

Vastgesteld op: 3 juli 2018

Inhoudsopgave

Privacybeleid	1
Privacyreglement	3
1. Wetgeving en definities	3
2. Reikwijdte	3
3. Verantwoordelijke	4
4. Verwerkingen	4
4.1 Doeleinden	4
4.2 Rechtmatige grondslag	4
4.3 Wijze van verwerking	5
4.4 Beveiliging	5
4.5 Doorgifte en samenwerken	5
4.6 Inzet van camera's	6
5. Transparantie en communicatie	6
5.1 Wet openbaarheid van bestuur	6
5.2 Wet hergebruik van overheidsinformatie	6
5.3 Informatieplicht	6
5.4 Rechten van betrokkenen	7
5.5 Indienen van verzoek	7
6. Plichten van de gemeente	7
6.1 Register van verwerkingen	7
6.2 Bewaartermijnen	8
6.3 Privacy by design en privacy by default	8
6.4 Privacy Impact Assessment	8
6.5 Datalekken	8
6.6 Functionaris voor gegevensbescherming	9
7. Taakverdeling	9
7.1 Rol en taken FG	9
7.2 Contactpersonen privacy	9
7.3 Privacy Officer	9
7.4 CISO	9
7.5 Rol en taken management en medewerkers	10

Privacybeleid en Privacyreglement gemeente Bergen op Zoom

Op 3 juli 2018 heeft het college het privacybeleid en het privacyreglement vastgesteld. Met het privacybeleid verduidelijkt het college aan welke principes de gemeente zich houdt bij de omgang met persoonsgegevens. Het privacyreglement is een verdieping van het beleid en laat zien hoe de gemeente met privacy, en met name de privacywetgeving, omgaat.

Privacybeleid gemeente Bergen op Zoom

Binnen de gemeente Bergen op Zoom wordt veel gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verzameld bij de burgers voor het goed uitvoeren van de gemeentelijke wettelijke taken. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met de persoonsgegevens omgaat. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen daarbij andere eisen aan de bescherming van gegevens en privacy. De gemeente is zich hier van bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

Het bestuur en management spelen een cruciale rol bij het waarborgen van privacy. De gemeente Bergen op Zoom geeft middels dit beleid een duidelijke richting aan privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente. En dit beleid is in lijn met het algemene beleid van de gemeente en de relevante lokale, regionale, nationale en Europese wet- en regelgeving.

Wettelijke kaders voor de omgang met gegevens

De gemeente is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Hiervoor gelden onder andere de volgende wettelijke kaders:

- Grondrechten op privéleven en de bescherming van persoonsgegevens: artikel 16 van het Verdrag betreffende de werking van de Europese Unie, artikel 7 en 8 van het Handvest van de grondrechten van de Europese Unie, artikel 8 Europees Verdrag voor de Rechten van de Mens en artikel 10 van de Nederlandse Grondwet;
- Algemeen kader voor de uitvoering: de Europese Algemene Verordening Gegevensbescherming (AVG) en de Nederlandse Uitvoeringswet Algemene Verordening Gegevensbescherming;
- Bijzondere nationale wetten zoals de Wet basisregistraties personen, de Participatiewet, de Jeugdwet en de Wet maatschappelijke ondersteuning, en aanverwante (lokale) regelgeving, waarin, nadere, sectorspecifieke, bepalingen over het verwerken van persoonsgegevens zijn vastgelegd.

Uitgangspunten

De gemeente gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. De gemeente houdt zich hierbij aan de volgende uitgangspunten:

Rechtmatigheid, behoorlijkheid, transparantie

Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.

Grondslag en doelbinding (proportionaliteit)

Persoonsgegevens worden alleen met een rechtmatige grondslag verwerkt. De gemeente zorgt er daarbij voor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt en niet verder op een met die doeleinden onverenigbare wijze worden verwerkt.

Dataminimalisatie (subsidiariteit)

De gemeente verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

Bewaartermijn

Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven.

Integriteit en vertrouwelijkheid

De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt de gemeente voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid.

Delen met derden

In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt de gemeente afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet. De gemeente controleert deze afspraken regelmatig.

Rechten van betrokkenen

De gemeente honoreert alle rechten van betrokkenen.

Dit Privacybeleid is verder uitgewerkt in het hiernavolgend Privacyreglement. Het beleid en het reglement worden jaarlijks geëvalueerd en indien nodig herzien. Aanpassingen worden aangekondigd via de website en in de lokale media. De actuele versie van het beleid en het reglement zijn te vinden op de website van de gemeente.

Privacyreglement gemeente Bergen op Zoom

In dit Privacyreglement laat de gemeente Bergen op Zoom zien op welke manier zij dagelijks omgaat met persoonsgegevens en privacy, en wat er wettelijk wel en niet verantwoord is.

Privacy speelt een belangrijke rol in de relatie tussen de burger en de overheid en staat daarmee hoog op de bestuurlijke agenda. Gemeenten hebben de verantwoordelijkheid over persoonsgegevens en gegevensuitwisseling op alle terreinen waar ze actief zijn. Gemeenten zijn verplicht om zorgvuldig en veilig, proportioneel en vertrouwelijk om te gaan met het verzamelen, bewaren en beheren van persoonsgegevens van burgers. Dat geldt voor taken op het gebied van basisadministraties, openbare orde en veiligheid, en het sociaal domein. Goed en zorgvuldig omgaan met persoonsgegevens is een dagelijkse bezigheid van gemeenten. Het beschermen van de privacy is complex, en wordt steeds complexer door technologische ontwikkelingen, de decentralisaties, grote uitdagingen op het terrein van veiligheid en Europese wetgeving. Daarom vindt de gemeente het belangrijk om transparant te zijn over de manier waarop zij met persoonsgegevens omgaat, en de privacy waarborgt.

1. Wetgeving en definities

De Europese Verordening; de Algemene Verordening Gegevensbescherming (AVG), is op 25 mei 2018 in werking getreden, en regelt samen met de Nederlandse Uitvoeringswet, het algemeen juridisch kader voor de omgang met persoonsgegevens.

Voor de definitie van begrippen wordt verwezen naar artikel 4 AVG. Hier wordt een korte omschrijving gegeven van enkele belangrijke begrippen:

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

Persoonsgegevens: Alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals gezondheidsgegevens, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld; naam, adres, woonplaats, geboortedatum, enzovoort). Naast gewone persoonsgegevens kent de wet ook zogenaamde bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals bijvoorbeeld etnische achtergrond of politieke voorkeuren.

Verwerkingsverantwoordelijke: Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. In het kader van dit reglement is het uitgangspunt dat de gemeente verwerkingsverantwoordelijke is.

Verwerker: De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.

Verwerking: Een verwerking is alles wat je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, raadplegen, verstrekken aan een ander, en vernietigen.

Gegevensbeschermingseffectbeoordeling: Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit heet ook wel een Privacy Impact Assessment (PIA).

2. Reikwijdte

Het privacyreglement is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van de gemeente, oftewel op alle verwerkingen die onder verantwoordelijkheid van de gemeente plaatsvinden. Dit reglement vormt daarbij een uitwerking van de wettelijke regelgeving uit de AVG en is bedoeld als een handleiding voor de organisatie. Het geeft in het algemeen de regels en uitgangspunten voor de eerlijke, zorgvuldige en rechtmatige verwerking van persoonsgegevens.

3. Verantwoordelijke

De bestuursorganen van de gemeente zijn verantwoordelijk voor de verwerkingen die door of namens de gemeente worden uitgevoerd. De bestuursorganen van de gemeente zijn onder andere de burgemeester, het college van burgemeester en wethouders en de gemeenteraad.

4. Verwerkingen

De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen.¹ In de AVG valt onder een verwerking: verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending of op andere wijze ter beschikking stellen, samenbrengen, combineren, afschermen, wissen of vernietigen van gegevens. Uit deze opsomming blijkt dat alles wat de gemeente met een persoonsgegeven doet een verwerking is.

Wij verwerken als gemeente persoonsgegevens voor de uitvoering van wettelijke en publieke taken en om diensten te verlenen aan burgers en bedrijven. Het gaat bijvoorbeeld om diverse processen binnen het sociaal domein. Zoals de registraties voor het verstrekken van uitkeringen en Wmo-voorzieningen en de uitvoering van de Jeugdwet. Maar natuurlijk ook buiten het sociaal domein zoals de registraties voor omgevingsvergunningen en handhaving. Voor de uitvoering van diverse specifieke wetten zoals de Participatiewet, Wmo, Jeugdwet en de Wet basisregistraties personen zijn in die wetten vaak ook specifieke regels opgenomen voor het verwerken van persoonsgegevens. Deze regels zijn bij de uitvoering van deze wetten dan primair van toepassing. Daar waar niets in specifieke wetgeving is geregeld, is uiteraard steeds de AVG van toepassing.

4.1 Doeleinden

Volgens de wet mogen persoonsgegevens alleen verzameld worden als daarvoor vooraf een doel is vastgesteld.² Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. De verwerkingsdoelen geven dus antwoord op de vraag 'waarom' persoonsgegevens worden verwerkt. Een belangrijke eis daarbij is dat doelen vooraf specifiek geformuleerd moeten zijn. De doelen mogen dus niet te ruim en vaag omschreven zijn of achteraf bepaald worden. De gegevens mogen in principe ook niet voor andere doelen verwerkt 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. Voor de uitvoering van de hiervoor genoemde specifieke wetten, zoals bijvoorbeeld de Participatiewet, de Wmo en de Jeugdwet, zijn de doelen voor het verwerken vaak in de betreffende wet vastgelegd, evenals de persoonsgegevens die gevraagd en verwerkt mogen worden. Door de gemeente wordt het doel per verwerking vastgelegd in het register van verwerkingen (zie ook paragraaf 7.1).

4.2 Rechtmatige grondslag

De wet zegt dat er voor elke verwerking van persoonsgegevens een grondslag uit de wet van toepassing moet zijn.³ Dat betekent dat de verwerking alleen mag plaatsvinden als de verwerking kan worden gebaseerd op één van de volgende zes grondslagen:

- de betrokkene heeft **toestemming** gegeven voor de verwerking van zijn persoonsgegevens;
- de verwerking is noodzakelijk voor de **uitvoering van een overeenkomst** waarbij de betrokkene partij is;
- de verwerking is noodzakelijk om te voldoen aan een **wettelijke verplichting**;
- de verwerking is noodzakelijk om de **vitale belangen** van de betrokkene of een ander te beschermen (alleen bij een ernstige bedreigingen voor de gezondheid);
- de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag (**publiekrechtelijke taak**);
- de verwerking is noodzakelijk voor de behartiging van de **gerechtvaardigde belangen** van de gemeente of van een derde (bedrijfsactiviteiten zoals het voeren van een personeelsadministratie).

¹ Artikel 4 lid 2 AVG.

² Artikel 5 lid 1 sub b AVG.

³ Artikel 6 lid 1 AVG.

Voor alle grondslagen zal er altijd een noodzaak moeten zijn om die gegevens te verwerken. Of het verwerken van bepaalde gegevens noodzakelijk is, moet altijd gemotiveerd worden. Voor de gemeente zijn met name de verwerking op basis van een wettelijke verplichting en de verwerking voor de vervulling van een taak van algemeen belang relevant. De gemeente zal toestemming zelden als grondslag gebruiken voor de verwerking van gegevens. Tussen de gemeente en de burger bestaat namelijk een bepaalde afhankelijkheidsrelatie of wanverhouding zodat vaak niet volledig aan de eis kan worden voldaan dat toestemming 'vrijelijk' moet zijn gegeven. De grondslag gerechtvaardigd belang mag door de gemeente alleen worden gebruikt voor zover typische bedrijfsmatige handelingen (zoals een private partij) worden verricht, bijvoorbeeld het voeren van een personeelsadministratie. Voor de uitoefening van andere taken mag deze grondslag niet worden gebruikt en kan deze grondslag voor de gemeente dus nooit een reden zijn voor de verwerking van gegevens van burgers.

4.3 Wijze van verwerking

De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de wet, en op een zorgvuldige wijze. De wet gaat daarbij uit van proportionaliteit en subsidiariteit. Dit betekent dat persoonsgegevens alleen mogen 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 worden zoveel mogelijk verzameld bij de betrokkene zelf. De gemeente zorgt ervoor dat de persoonsgegevens die worden verwerkt kloppen. Deze gegevens worden verder alleen verwerkt door personen met een geheimhoudingsplicht. Die geheimhoudingsplicht geldt voor alle ambtenaren direct op grond van de Ambtenarenwet. Door de gemeente ingehuurde derden verklaren schriftelijk en voorafgaand aan hun inzet zich te houden aan dezelfde regels. Advocaten die optreden voor de gemeente hebben een geheimhoudingsplicht op grond van de Advocatenwet.

4.4 Beveiliging

De gemeente beveiligt alle persoonsgegevens. Dit moet onder meer voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. Hoe de gemeente dit doet staat in het informatiebeveiligingsbeleid van de gemeente en in een eventueel aanvullend beveiligingsbeleid specifiek opgesteld voor een proces of registratie. Het Informatiebeveiligingsbeleid 2017-2020 van de gemeente is in 2017 geactualiseerd en vastgesteld door het college van burgemeester en wethouders. Het informatiebeveiligingsbeleid is volledig in lijn met de geldende gemeentelijke beveiligingsnormen zoals vastgelegd in de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) van VNG Realisatie/IBD.

In de BIG staan verschillende technische en organisatorische maatregelen genoemd om persoonsgegevens te beveiligen tegen uiteenlopende risico's zoals ongeautoriseerde toegang tot data, verlies van data of gijzeling van data (ransomware). De gemeente heeft in het informatiebeveiligingsbeleid onder andere vastgelegd hoe wordt omgegaan met het toekennen van autorisaties tot systemen. Het autorisatiebeleid houdt in dat vooraf is vastgelegd welke functie toegang moeten hebben tot welke systemen, dossiers en gegevens. Daarmee krijgen medewerkers toegang tot informatie die noodzakelijk is voor de uitoefening van hun taak en dus niet tot andere gegevens. Zo zijn medewerkers van Team Burgerzaken geautoriseerd tot de Basis Registratie Personen (BRP), maar dat geldt niet voor bijvoorbeeld medewerkers van Team P&O.

Wat per verwerkingsproces een passend beschermingsniveau is voor beveiliging wordt mede bepaald door het soort persoonsgegeven, bijvoorbeeld een bijzonder persoonsgegeven, de mate van beschikbaarheid en toepasbaarheid van de beveiligingsmaatregel, de kosten die verbonden zijn aan de maatregel in relatie tot de kans op het risico en de gevolgen voor betrokkenen indien de persoonsgegevens openbaar worden of juist vernietigd zijn. Persoonsgegevens worden versleuteld verzonden bijvoorbeeld door gebruik te maken van Gemnet, Zorgmail of andere beveiligde diensten waarmee informatie kan worden verzonden.

4.5 Doorgifte en samenwerken

Onder doorgifte wordt bijvoorbeeld verstaan het opslaan in de cloud bij of het anderszins ter beschikking stellen van persoonsgegevens aan een organisatie. Persoonsgegevens mogen in principe niet worden doorgegeven aan een organisatie in een land buiten de EU. Dit komt omdat binnen de EU een goede bescherming voor persoonsgegevens geldt, en daarbuiten niet in alle gevallen. De gemeente geeft dan ook alleen

persoonsgegevens door aan een land buiten de Europese Economische Ruimte of een internationale organisatie op grond van goedgekeurde afspraken door de Europese Commissie.

Met organisaties die persoonsgegevens verwerken in onze opdracht of samenwerkingsverbanden in de regio maken wij altijd schriftelijke afspraken om te zorgen voor eenzelfde niveau van beveiliging en vertrouwelijkheid van gegevens. De gemeente blijft daarbij verantwoordelijk voor deze verwerkingen. Schriftelijke afspraken worden in de regel vastgelegd in een zogenaamde verwerkersovereenkomst. De gemeente maakt daarbij gebruik van de modelverwerkersovereenkomst van de IBD om een uniforme kwaliteit te garanderen. De eisen die in dit model zijn opgenomen worden ook bij aanbestedingen in aanmerking genomen.

4.6 Inzet van camera's

Binnen de gemeente wordt onder bepaalde omstandigheden gebruik gemaakt van cameratoezicht, zoals vastgelegd in de Gemeentewet.⁴ Cameratoezicht wordt onder andere gebruikt voor het vergroten van de veiligheid op straat. Camera's kunnen een grote inbreuk maken op de privacy van diegene 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. Als er gebruik wordt gemaakt van cameratoezicht dan zal dit voor het publiek duidelijk kenbaar worden gemaakt aan een ieder die de desbetreffende openbare plaats betreedt.

5. Transparantie en communicatie

5.1 Wet openbaarheid van bestuur (Wob)

Via de Wob (en straks wellicht de Wet open overheid die de Wob op den duur moet vervangen) kan een verzoek om informatie worden ingediend 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 hierbij geen persoonsgegevens verstrekt.⁵

5.2 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 hierbij geen persoonsgegevens verstrekt.

5.3 Informatieplicht

De gemeente informeert betrokkenen over het verwerken van persoonsgegevens en hun rechten.⁶ Wanneer betrokkenen gegevens aan de gemeente geven, worden zij op de hoogte gesteld van de manier waarop de gemeente met persoonsgegevens om zal gaan. In het algemeen worden betrokkenen hierover geïnformeerd via de privacyverklaring op de website. Meer specifiek per verwerking is deze informatie beschikbaar op het moment dat er een verwerking gaat plaatsvinden en/of klantcontact is, onafhankelijk of dit in persoon is of digitaal. Informatie kan bijvoorbeeld via aanvraagformulieren worden verstrekt. Vaak staat op de aanvraagformulieren al vermeld welke gegevens zonder toestemming niet openbaar gemaakt zullen worden. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de gemeente persoonsgegevens van hem/haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt. Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze verder worden verwerkt.

⁴ Artikel 151c Gemeentewet.

⁵ Artikel 10 lid 1 onder d en artikel 10 lid 2 onder e Wob.

⁶ Artikel 13 en 14 AVG.

5.4 Rechten van betrokkenen

De wet bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt.⁷ Deze rechten worden ook wel de rechten van betrokkenen genoemd, en bestaan uit de volgende rechten:

- Recht op informatie: Betrokkenen hebben het recht om aan de gemeente te vragen of en waarom persoonsgegevens worden verwerkt.
- Recht op inzage: Betrokkenen hebben de mogelijkheid om de persoonsgegevens die worden verwerkt in te zien en hiervan een kopie te krijgen. De betrokkene hoeft hiervoor geen reden op te geven maar hij mag niet overdreven veel verzoeken in korte tijd indienen.
- Recht op rectificatie (correctie): Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren.
- Recht om vergeten te worden: Behoudens wettelijke beperkingen heeft betrokkene het recht om persoonsgegevens te laten verwijderen, bijvoorbeeld wanneer de toestemming hiervoor is ingetrokken en er geen andere rechtsgrond bestaat voor de verwerking.
- Recht op bezwaar: Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van persoonsgegevens. De gemeente zal aan bezwaren tegemoetkomen, tenzij er gerechtvaardigde gronden zijn voor de verwerking en/of de wet voorschrijft dat de gemeente de gegevens verwerkt.

5.5 Indienen van verzoek

Om gebruik te maken van de hiervoor genoemde rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als elektronisch (via e-mail of gemeentelijke website) ingediend worden. De gemeente heeft één maand de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Deze termijn kan indien nodig met twee maanden worden verlengd. De gemeente zal binnen de wettelijke termijn laten weten wat er met het verzoek gaat gebeuren. Als het verzoek niet wordt opgevolgd is er de mogelijkheid om bezwaar te maken bij de gemeente. Als betrokkene vermoedt dat persoonsgegevens worden verwerkt in strijd met de wet kan ook een klacht worden ingediend bij de Autoriteit Persoonsgegevens (AP). Aan de hand van een verzoek kan de gemeente aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene. De verzoeker kan bijvoorbeeld worden gevraagd om zich persoonlijk bij de gemeente te identificeren met een wettelijk identificatiebewijs. Voor een elektronisch verzoek via de website kan bijvoorbeeld een e-formulier met DigiD worden gebruikt.

6. Plichten van de gemeente

6.1 Register van verwerkingen

De gemeente is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan de gemeente de verwerkingsverantwoordelijke is.⁸ Elk register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, namelijk:

- De naam en contactgegevens van de gemeente en van de FG;
- De doelen en de grondslag van de verwerking;
- Een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- Een beschrijving van met wie de gegevens worden gedeeld;
- De termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
- Een algemene beschrijving van de beveiligingsmaatregelen.

De gemeente zorgt voor een actueel en volledig register van verwerkingen. De FG speelt een leidende rol bij het opzetten van de daarvoor benodigde structuur. Op verzoek van de AP dient deze administratie overhandigd te kunnen worden ter controle. Een publieksversie van het register zal door de gemeente ook actief openbaar gemaakt worden via de website.

⁷ Artikel 13 t/m 20 AVG.

⁸ Artikel 30 AVG.

6.2 Bewaartermijnen

De gemeente bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van gemeentelijke taken, of zoals vastgelegd in de Archiefwet. De hoofdregel is: bewaren mag zolang het nodig is voor het doel van de verwerking of wettelijk is verplicht. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel en waarvoor geen wettelijk bewaartermijn is vastgesteld, worden deze zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens vernietigd worden, of zo worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren. Uitgangspunt bij het vaststellen van bewaartermijnen is de selectielijst op grond van de Archiefwet.⁹

6.3 Privacy by design and default

Bij het verwerken van persoonsgegevens zijn op grond van de AVG de beginselen van gegevensbescherming door ontwerp (privacy by design) en gegevensbescherming door standaardinstellingen (privacy by default) van toepassing.¹⁰ Privacy by design houdt in dat de gemeente al bij het ontwerpen van een nieuw systeem of een nieuwe werkwijze ervoor zorgt dat persoonsgegevens goed worden beschermd en betrokkenen hun rechten goed kunnen uitoefenen. Bijvoorbeeld door onder andere de toegang tot de persoonsgegevens goed te regelen en ervoor te zorgen dat persoonsgegevens zo nodig automatisch worden versleuteld of verwijderd. Privacy by default houdt in dat de gemeente technische en organisatorische maatregelen neemt om ervoor te zorgen dat, als standaard, alléén die persoonsgegevens worden verwerkt die noodzakelijk zijn voor het specifieke doel. Bijvoorbeeld door bij de aanmelding voor een nieuwsbrief niet meer gegevens te vragen dan nodig (dataminimalisatie). Privacy by design en privacy by default worden ook bij aanbestedingen in aanmerking genomen.

6.4 Privacy Impact Assessment

Met een Privacy Impact Assessment (PIA), ofwel een gegevensbeschermingseffectbeoordeling, worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy.¹¹ De gemeente voert deze in ieder geval uit wanneer er een geautomatiseerde verwerking, een grootschalige verwerking, of wanneer er een grootschalige monitoring van openbare ruimten plaatsvindt. Verder zal in het bijzonder bij nieuwe verwerkingen waarbij bijzondere persoonsgegevens worden verwerkt en/of waarbij nieuwe technologieën worden gebruikt een PIA worden uitgevoerd. Bij het uitvoeren van de PIA wordt de Functionaris Gegevensbescherming (FG) advies gevraagd. De uitkomsten van een PIA worden gemotiveerd betrokken bij de beslissing voor het al dan niet aanvangen van de verwerking. Dat betekent dat altijd gemotiveerd wordt beargumenteerd welke keuzes worden gemaakt ten aanzien van de verwerking van persoonsgegevens. De keuzes zijn daarmee transparant en onder andere voor de FG, de gemeenteraad of de nationaal toezichthouder beschikbaar voor het uitoefenen van hun (controleerende) taken.

6.5 Datalekken

We spreken van een datalek wanneer sprake is van een inbreuk op de beveiliging van persoonsgegevens door blootstelling aan verlies of onrechtmatige verwerking.¹² Een beveiligingsincident wordt altijd gemeld bij de FG. Wanneer er een datalek heeft plaatsgevonden met een risico voor de rechten en vrijheden van personen meldt de gemeente dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, aan de AP. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval meldt de gemeente dit ook aan de betrokkenen in eenvoudige en duidelijke taal. Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd. De gemeente houdt een overzicht bij van alle datalekken en de getroffen maatregelen.

⁹ Op grond van de Archiefwet worden selectielijsten gemaakt waarin wordt beschreven welke informatie op welke termijn moet worden vernietigd en welke informatie permanent bewaard moet worden. Zie artikel 5 Archiefwet.

¹⁰ Artikel 25 AVG.

¹¹ Artikel 35 AVG.

¹² Artikel 33 en 34 AVG.

6.6 Functionaris voor gegevensbescherming (FG)

De gemeente heeft een FG aangesteld en aangemeld bij de Autoriteit Persoonsgegevens (AP).¹³ 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 het AP. Voor het uitoefenen van toezicht heeft de FG controlebevoegdheden. De FG is eveneens contactpersoon voor burgers voor vragen over privacy en het uitoefenen van rechten. De FG neemt geen taken op het gebied van bescherming van de privacy over van de teams. De teams hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens. Een verwerking van persoonsgegevens wordt eerst aan de FG gemeld voordat de verwerking begint of verder gaat. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en het gemeentelijk beleid op het gebied van privacy. De rol en taken van de FG zijn nader uitgewerkt in het Reglement Functionaris voor de gegevensbescherming. Voor vragen op het gebied van privacy kan contact worden opgenomen met de FG via: FG@bergenopzoom.nl. De contactgegevens van de FG zijn voor burgers ook gepubliceerd op de website van de gemeente.

7. Taakverdeling

7.1 Rol en taken FG

De rol en taken van de FG zijn hiervoor omschreven en nader uitgewerkt in het Reglement Functionaris voor de gegevensbescherming.

7.2 Contactpersonen privacy

Het uitgangspunt is dat er een contactpersoon privacy is per team. In ieder geval worden er contactpersonen privacy aangewezen voor de teams Concernstaf, ISD, Jeugd/CJG, Maatschappij, P&O, Publieksdiensten,¹⁴ Veiligheid, Handhaving & Toezicht en Wmo. Binnen deze teams vormt het verwerken van persoonsgegevens immers een belangrijk en/of gevoelig onderdeel bij het uitvoeren van de taken. De contactpersoon privacy kan binnen het team fungeren als het aanspreekpunt voor advies over de verwerking van persoonsgegevens en de uitleg van de AVG. De contactpersoon privacy is tevens de schakel naar en het aanspreekpunt van de FG en de Privacy Officer voor bijvoorbeeld de registratie van nieuwe of gewijzigde verwerkingen en het behandelen van verzoeken van burgers die betrekking hebben op de uitoefening van hun rechten.

7.3 Privacy Officer

Naast de contactpersonen wordt er een Privacy Officer aangewezen. Deze vormt een belangrijk onderdeel van de governance van gegevensbescherming binnen de gemeente. De Privacy Officer is bekend met en heeft kennis van de verschillende systemen binnen de gemeente waarin persoonsgegevens worden verwerkt en heeft als taak organisatiebreed te adviseren over de aanschaf en inrichting van systemen. Vanuit een meer technische achtergrond kan hij de FG, de contactpersonen en de organisatie adviseren over gegevensbescherming. Daarnaast worden meer centrale uitvoerende taken op het gebied van privacy zo veel mogelijk bij de Privacy Officer belegd zodat de FG primair zijn adviserende en toezichthoudende rol kan vervullen. Denk bijvoorbeeld aan de feitelijke implementatie van privacymaatregelen (wijzigingen in procesuitvoering en bedrijfsvoering), het bijhouden van het register van verwerkingen en ondersteuning bij het opstellen van verwerkersovereenkomsten en gegevensbeschermingseffectrapportages.

7.4 CISO

De verwerking van persoonsgegevens is onlosmakelijk verbonden met de beveiliging daarvan. Beveiliging van persoonsgegevens is een verantwoordelijkheid van iedere medewerker. Maar om er voor te zorgen dat er een samenhangend pakket aan maatregelen in de gemeente beschikbaar is ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen een gemeente is er de CISO; Chief Information Security Officer. De CISO zal in samenwerking met de FG en de Privacy Officer toezicht houden op en adviseren over de beveiliging van persoonsgegevens binnen de organisatie.

¹³ Artikel 37 t/m 39 AVG.

¹⁴ Op grond van de wet Basis Registratie Personen (BRP) is voor de BRP reeds een privacy beheerder aangesteld. Deze rol zal worden verdisconteerd in de rol van contactpersoon

7.5 Rol en taken management en medewerkers

Management en medewerkers zijn verantwoordelijk voor een zorgvuldige omgang met persoonsgegevens. Bij de uitvoering van hun taken zijn zij zich bewust van het feit dat privacy in de operationele processen geborgd moet zijn en de mogelijke inbreuk die kan worden gemaakt op de persoonlijke levenssfeer van betrokkenen. Dit betekent dat zij handelen naar het privacybeleid en privacyreglement van de gemeente, de interne procedures ten aanzien van beheer en beveiliging volgen (bijvoorbeeld over toegang tot en verwijdering van persoonsgegevens) en geen persoonsgegevens gebruiken waarover de gemeente als publiek orgaan beschikt voor privaatrechtelijke taken.

Medewerkers worden door middel van opleiding, training en/of interne voorlichting opgeleid zodat zij beschikken over kennis op basisniveau over gegevensbescherming. Medewerkers zijn daarmee in staat te handelen in overeenstemming met toepasselijke regelgeving en situaties te herkennen waarin expertise nodig is van de FG. Uiteraard zijn ze daarmee eveneens in staat betrokkenen goed te informeren over hun rechten.

Afsluiting

Als de gemeente een wettelijke verplichting niet nakomt kan de betrokkene een klacht indienen. Deze zal via de algemene klachtenregeling worden behandeld. In gevallen waar het reglement niets over zegt, beslist het verantwoordelijke bestuursorgaan van de gemeente. Een klacht wordt ook altijd doorgegeven aan de FG en de FG wordt eveneens betrokken bij de besluitvorming hieromtrent.