

Privacybeleid en -reglement voor gemeente Beek 2023-2025

Inhoud

1. Privacybeleid gemeente Beek 4
 - Inleiding 4
 - Wettelijke kaders voor de omgang met gegevens 4
 - Uitgangspunten 5
2. Privacyreglement gemeente Beek 7
 1. Wetgeving en definities 7
 2. Reikwijdte 7
 3. Verantwoordelijke 8
 4. Verwerkingen 8
 5. Transparantie en communicatie 9
 6. Geautomatiseerde verwerkingen 10
 7. Plichten van de gemeente 11

Voorwoord

Dit privacybeleid en -reglement is van toepassing op de verwerking van persoonsgegevens conform de Algemene Verordening Gegevensbescherming en de Wet politiegegevens. Dit is nieuw t.o.v. het vorige privacy beleid.

Het privacybeleid is een kader waarin wordt aangegeven aan welke principes de gemeente Beek zich houdt.

Het privacyreglement is een verdieping van het beleid en laat zien hoe de gemeente met privacy, en met name de wet, omgaat. Met andere woorden: hoe wordt het beleid in de praktijk uitgevoerd?

De privacyverklaring is een apart document dat specifiek bedoeld is voor de gemeentelijke website. Uiteraard komen daarin ook weer elementen terug uit het privacy beleid en het privacyreglement.

1. Privacybeleid gemeente Beek

Inleiding

Binnen de gemeente Beek 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. In deze tijd gaat ook de gemeente mee met nieuwe ontwikkelingen. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen 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 Beek 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. Dit privacybeleid van gemeente Beek is in lijn met het algemene beleid van de gemeente en de relevante lokale, regionale, nationale en Europese wet- en regelgeving.

Dit beleid is van toepassing op de verwerking van persoonsgegevens conform de Algemene Verordening Gegevensbescherming en de Wet politiegegevens.

De werkgever van de boa is verantwoordelijk voor de verwerking van persoonsgegevens volgens de Memorie van Toelichting bij de wetswijziging. Verder is in de EU-richtlijn 2018/680, waarop de Wpg is

gebaseerd, aansluiting gezocht bij de AVG. De verwerking van persoonsgegevens in het kader van opsporingstaken door buitengewoon opsporingsambtenaren (boa's) valt niet onder de Algemene Verordening gegevensbescherming (AVG), maar in plaats daarvan onder de Wet politiegegevens (Wpg). Daarmee ontstaat er één wettelijk regime voor de verwerking van persoonsgegevens in de strafrechtelijke keten.

Verplichtingen uit de AVG zoals de meldplicht datalekken, rechten van betrokkenen en het uitvoeren van DPIA's gelden ook voor de Wpg. De hiervoor vastgestelde interne procedures worden naar analogie van de AVG toegepast, behalve voor de gevallen waarin de Wpg van de AVG afwijkt.

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:

- De Algemene Verordening Gegevensbescherming (AVG)
- De Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)
- Wet Politiegegevens (Wpg)
- Besluit Politiegegevens boa (Bpg boa)

Daar waar in dit beleid gesproken wordt over persoonsgegevens wordt tevens bedoeld politiegegevens in de zin van Wpg.

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 (artikel 5.1.a AVG en artikel 3 Wpg)

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

Doelbinding en grondslag (artikel 5.1.b en 6 AVG en artikel 8, 9 en 13 Wpg)

De gemeente zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtmatige grondslag verwerkt.

Minimale gegevensverwerking/noodzakelijkheid (artikel 5.1.c AVG en artikel 4 Wpg)

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

Juistheid (artikel 5.1.d AVG en artikel 4 Wpg)

De gemeente zorgt ervoor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden. Deze gegevens worden alleen verwerkt door personen met een geheimhoudingsplicht. Daarnaast beveiligd de gemeente alle persoonsgegevens. Dit moet 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 onze gemeente.

Opslagbeperking (artikel 5.1.e AVG en artikel 14 Wpg)

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 (artikel 5.1.f AVG en artikel 4a Wpg)

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.

De verwerkingsverantwoordelijke en de verwerker treffen passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking van persoonsgegevens wordt verricht in overeenstemming met hetgeen in de wet is bepaald en om een beveiligingsniveau te waarborgen dat op het risico is afgestemd.

Delen met derden (AVG)

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 periodiek.

Ter beschikking stellen (artikel 15 Wpg)

'Free flow of information', in principe worden politiegegevens gedeeld met eenieder die de gegevens noodzakelijk heeft voor de uitoefening van zijn taak. De Wpg kent een gesloten verstrekkingenregime, wat betekent dat in de Wpg staat aan wie de Boa gegevens mag verstrekken.

Het Wpg domein bestaat uit: politie, marechaussee, rijksrecherche, Bijzondere Opsporingsdiensten* (BOD), boa's.

Verstrekken (artikel 7, 6 Bpg, artikel 16 t/m 24 Wpg)

Het delen van politiegegevens buiten het Wpg domein, (bijvoorbeeld aan bureau Halt, belastingdienst, Centraal Justitieel Incassobureau) kan onder voorwaarde.

Subsidiariteit (AVG en Wpg)

Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt.

Proportionaliteit (AVG en Wpg)

De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel.

Rechten van betrokkenen (AVG en Wpg)

De gemeente honoreert alle rechten van betrokkenen.

Privacy audits (artikel 6.1 lid 1 Bpg)

Er bestaat een verplichting tot externe privacy-audit met rapportage aan de Autoriteit Persoonsgegevens (AP), twee jaar na inwerkingtreding en daarna elke 4 jaar. Daarnaast dient er ieder jaar een interne audit te worden uitgevoerd.

Privacy by design (art 25 AVG, art 4a Wpg)

Vanaf de ontwikkeling van producten en diensten is er aandacht voor privacy en wordt er gebruik gemaakt van privacy-verhogende maatregelen en wordt bijvoorbeeld gekeken naar de benodigde technische en organisatorische maatregelen.

Privacy by default (art 25 AVG, art 4a Wpg)

Het concept van Privacy by Default verplicht organisaties om de privacy van belanghebbenden te beschermen door de instellingen en functies van de producten of diensten standaard (by default) op de meest privacy vriendelijke stand te zetten. Voor de gemeente Beek geldt dat voor een nieuwe verwerking of een wijziging in een bestaande verwerking een gegevensbeschermingseffectbeoordeling (DPIA-Toets) uitgevoerd dient te worden.

Dit privacybeleid wordt door het college van burgemeesters en wethouders vastgesteld voor een periode van twee jaar. Het beleid wordt periodiek geëvalueerd en indien nodig herzien. De meest actuele versie van het beleid is te vinden op www.gemeentebEEK.nl. Dit privacybeleid treedt in werking na bekendmaking.

2. Privacyreglement gemeente Beek

In dit reglement laat gemeente Beek zien op welke manier zij dagelijks omgaat met persoonsgegevens, politiegegevens 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

*) 1. FIOD (Fiscale Inlichtingen- en Opsporingsdienst), valt onder het ministerie van Financiën;

2. ISZW-DO (Inspectie Sociale Zaken en Werkgelegenheid, Directie Opsporing), valt onder het ministerie van Sociale Zaken en Werkgelegenheid;

3. NVWA-IOD (Nederlandse Voedsel- en Warenautoriteit, Inlichtingen- en Opsporingsdienst), valt onder het ministerie van Economische Zaken;

4. ILT-IOD (Inspectie Leefomgeving en Transport, Inlichtingen- en Opsporingsdienst), valt onder het ministerie van Infrastructuur en Milieu.

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 nieuwe Europese wetgeving. Daarom vinden wij het belangrijk om transparant te zijn over de manier waarop wij met persoonsgegevens omgaan, en de privacy waarborgen.

1. Wetgeving en definities

De Algemene Verordening Gegevensbescherming (AVG) zorgt, samen met de uitvoeringswet, onder andere voor versterking en uitbreiding van de privacyrechten met meer verantwoordelijkheden voor organisaties. De volgende begrippen worden in de AVG gebruikt (Artikel 4, AVG) en gelden ook voor de Wpg en lichten we hieronder wat nader toe:

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

Persoonsgegevens: Alle gegevens die gaan over betrokkenen en waarmee je een betrokkene als individu kunt identificeren. Het gaat hierbij om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld; naam, adres, geboortedatum). Naast gewone persoonsgegevens kennen we ook gevoelige persoonsgegevens, zoals het Burgerservicenummer (BSN) en bijzondere persoonsgegevens. Dit zijn gegevens die gaan over extra gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren of gezondheid.

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 Data Protection Impact Assessment (DPIA).

Verwerkingsverantwoordelijke: Een persoon of organisatie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

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

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

Politiegegeven: Een persoonsgegeven dat verwerkt wordt in het kader van de opsporingstaak. Hiervoor geldt de Wpg. Een politiegegeven is een specifieke versie van een persoonsgegeven.

2. Reikwijdte

Het reglement is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van de gemeente. Oftewel: voor alle verwerkingen die binnen de gemeente plaatsvinden.

3. Verantwoordelijke

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.

4. Verwerkingen

De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen. Onder een verwerking valt:

- Verzamelen, vastleggen en ordenen
- Bewaren, bijwerken en wijzigen
- Opvragen, raadplegen, gebruiken
- Verstrekken door middel van doorzending
- Verspreiding of enige andere vorm van ter beschikkingstellen
- Samenbrengen, met elkaar in verband brengen
- Afschermen, uitwissen of vernietigen van gegevens

Uit deze opsomming blijkt dat alles wat je met een persoonsgegeven doet een verwerking is.

Doelinden (Artikel 5, AVG, artikel 3 Wpg)

Volgens de wet mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. De gegevens mogen niet voor andere doelen verwerkt worden. Voor de uitvoering van sommige wetten, zoals bijvoorbeeld de Jeugdwet,

zijn de doelen voor het verwerken in de wet al vastgelegd, net als de persoonsgegevens die gevraagd en verwerkt mogen worden.

Rechtmatige grondslag (Artikel 6, AVG, artikel 3 Wpg)

De wet zegt dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag van toepassing moet zijn. Dat betekent dat de verwerking alleen mag plaatsvinden:

- Om een verplichting na te komen die in de wet staat
- Voor de uitvoering van een overeenkomst waarbij de betrokkene partij is
- Om een ernstige bedreiging voor het leven of de gezondheid van de betrokkene te bestrijden
- Voor de goede vervulling van de gemeentelijke taak
- Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking
- Als de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de gemeente.

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. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. 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 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.

Juistheid (Artikel 5 AVG, artikel 4 Wpg)

De gemeente zorgt ervoor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden. Deze gegevens worden alleen verwerkt door personen met een geheimhoudingsplicht.

Daarnaast beveiligt de gemeente alle persoonsgegevens. Dit moet 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 beveiligingsplan specifiek opgesteld voor een proces of registratie.

Doorgifte (Artikel 44 t/m 50, AVG)

De gemeente geeft geen persoonsgegevens door aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie.

Ter beschikking stellen (artikel 15 Wpg)

'Free flow of information', in principe worden politiegegevens gedeeld met eenieder die de gegevens noodzakelijk heeft voor de uitoefening van zijn taak. De Wpg kent een gesloten verstrekkingenregime, wat betekent dat in de Wpg staat aan wie de Boa gegevens mag verstrekken.

Het Wpg domein bestaat uit: politie, marechaussee, rijksrecherche, Bijzondere Opsporingsdiensten (BOD)*, boa's.

Verstrekken (artikel 6, 7, 16 t/m 24 Wpg)

Het delen van politiegegevens buiten het Wpg domein, kan onder voorwaarde.

5. Transparantie en communicatie

Wet open overheid

Via 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.

*) 1. FIOD (Fiscale Inlichtingen- en Opsporingsdienst), valt onder het ministerie van Financiën;

2. ISZW-DO (Inspectie Sociale Zaken en Werkgelegenheid, Directie Opsporing), valt onder het ministerie van Sociale Zaken en Werkgelegenheid;

3. NVWA-IOD (Nederlandse Voedsel- en Warenautoriteit, Inlichtingen- en Opsporingsdienst), valt onder het ministerie van Economische Zaken;

4. ILT-IOD (Inspectie Leefomgeving en Transport, Inlichtingen- en Opsporingsdienst), valt onder het ministerie van Infrastructuur en Milieu.

Informatieplicht (Artikel 13 en 14, AVG, art 24 Wpg)

De gemeente informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de gemeente geven, worden zij op de hoogte gesteld van de manier waarop de gemeente met persoonsgegevens om zal gaan. Dit kan bijvoorbeeld via een formulier gebeuren. Vaak staat op de aanvraagformulieren 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 voor de eerste keer worden verwerkt.

Bewaartermijn

De gemeente bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van gemeentelijke taken, of zoals vastgelegd in de Archiefwet. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel 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.

Rechten van betrokkenen (Artikel 13 t/m 20 AVG, art 24 t/m 28 Wpg)

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.

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 zijn/haar persoonsgegevens worden verwerkt.
- **Inzagerecht:** Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt.
- **Correctierecht:** Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren
- **Recht van verzet:** Betrokkenen hebben het recht aan de gemeente te vragen om hun persoonsgegevens niet meer te gebruiken.
- **Recht om vergeten te worden:** In bepaalde in de AVG opgesomde gevallen, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen.
- **Recht op overdraagbaarheid van gegevens:** Betrokkenen hebben het recht om de door hen aan de gemeente verstrekte persoonsgegevens in een gestructureerde, gangbare en machinaal leesbare vorm te verkrijgen en aan een andere verwerkingsverantwoordelijke te laten overdragen. (niet van toepassing binnen Wpg)
- **Recht op bezwaar:** Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens. De gemeente zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

Indienen van verzoek

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als via de e-mail ingediend worden. De gemeente heeft vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Binnen vier weken zal de gemeente 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, of een klacht in te dienen 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.

6. Geautomatiseerde verwerkingen

Profilering

Gemeente Beek maakt geen gebruik van profilering.

Big data onderzoek en tracking

Gemeente Beek maakt geen gebruik van Big data en tracking.

Inzet van camera's handhaving openbare orde

Binnen de gemeente wordt onder bepaalde omstandigheden gebruik gemaakt van cameratoezicht, zoals vastgelegd in de Gemeentewet (artikel 151c). Cameratoezicht wordt onder andere gebruikt voor het vergroten van de veiligheid op straat, ten behoeve van het toezicht op een openbare plaats. 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.

Het gebruik van camera's door particulieren op de openbare weg is alleen mogelijk met expliciete toestemming van het college van B&W. Daarvoor wordt er een convenant afgesloten tussen de particulieren en het bestuursorgaan waarin o.a. de grondslag, het doel, de maatregelen tegen verlies, en de bewaartermijn in opgenomen worden.

Gemeente Beek zal zelf alleen gebruik maken van cameratoezicht onder de voorwaarden zoals opgenomen in artikel 151c van de gemeentewet. Voor het gebruik van camera's op de openbare weg door particulieren wordt altijd een convenant afgesloten.

Inzet van camera's in en rondom gemeentelijke gebouwen

Cameratoezicht is een ondersteunend middel voor de bescherming van medewerkers en bezoekers en voor de beveiliging van eigendommen en maakt deel uit van een breed pakket aan maatregelen. Er moet sprake zijn van een gerechtvaardigd belang, het moet noodzakelijk zijn en een gegevensbeschermingseffectbeoordeling (DPIA) is noodzakelijk.

7. Plichten van de gemeente

Register van verwerkingen (Artikel 30, AVG, artikel 31 Wpg)

De gemeente is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan de gemeente de verwerkingsverantwoordelijke is. 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 verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke verwerkingsverantwoordelijke;
- De doelen van de verwerking;
- Een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- Een beschrijving van de ontvangers van de persoonsgegevens;
- Een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
- De termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
- Een algemene beschrijving van de beveiligingsmaatregelen.

Gegevensbeschermingseffectbeoordeling (Artikel 35, AVG, artikel 4c Wpg)

Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. De gemeente voert deze uit wanneer er een geautomatiseerde verwerking, een grootschalige verwerking, of wanneer er een grootschalige monitoring van openbare ruimten plaatsvindt. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt.

Aanstellen Functionaris voor gegevensbescherming (FG) (Artikel 37 t/m 39, AVG, artikel 36 Wpg)

De gemeente heeft een FG aangesteld. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de functionaris zijn informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van de AP. Het is niet de bedoeling dat de functionaris 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. Een verwerking van persoonsgegevens wordt eerst aan de FG gemeld voordat de verwerking begint. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en de gemeentelijke richtlijnen op het gebied van privacy.

Voor vragen over privacy of over deze toelichting kunt u contact opnemen met de functionaris voor gegevensbescherming van gemeente Beek via: functionarisgegevensbescherming@gemeentebek.nl

Gegevensbeschermingseffectbeoordeling (DPIA)(art 35 AVG, art. 4c Wpg)

De gemeente is voortdurend in ontwikkeling. Zo worden processen en systemen periodiek aangepast of nieuw aangeschaft. Daardoor kan er sprake zijn van een nieuwe verwerking of wijziging van een bestaande verwerking. In de AVG en Wpg is op hoofdlijnen aangegeven wanneer een DPIA verplicht is. Dat is het geval als een gegevensverwerking waarschijnlijk een hoog privacy risico oplevert voor de betrokkenen van wie de organisatie gegevens verwerkt.

Datalekken (Artikel 33 en 34, AVG, art 33 Wpg)

We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben. Wanneer er een datalek heeft plaatsgevonden meldt de gemeente dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, aan de AP, tenzij het niet waarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van de betrokkenen inhoudt. 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.

Afsluiting

Als de gemeente een wettelijke verplichting niet nakomt kan de betrokkene een klacht indienen. Deze zal via de klachtenregeling van de gemeente worden behandeld. In gevallen waar het reglement niets over zegt, beslist het verantwoordelijke bestuursorgaan van de gemeente.

Dit product is een eenvoudige en begrijpbare vertaling van de huidige privacywetgeving en gebaseerd op de AVG en Wpg. Vanzelfsprekend is de toepasbare wet- en regelgeving altijd leidend en kunnen er geen rechten ontleend worden aan dit document.