



## **Privacyregeling Wet politiegegevens gemeente Bernheze**

**Vastgesteld door het college op: 8 augustus 2023**



Heb oog voor privacy  
en informatieveiligheid

# Inhoud

<b>Definities .....</b>	<b>3</b>
<b>1. Inleiding.....</b>	<b>4</b>
<b>2. Doelen .....</b>	<b>4</b>
<b>3. Scope .....</b>	<b>4</b>
<b>4. Wettelijke verplichtingen.....</b>	<b>4</b>
<b>5. Informatiebeveiliging.....</b>	<b>5</b>
<b>6. Functionaris gegevensbescherming .....</b>	<b>5</b>
<b>7. Rechten van betrokkenen.....</b>	<b>5</b>
<b>8. Het bewaren, verwijderen en vernietigen van politiegegevens .....</b>	<b>6</b>
<b>9. Het ter beschikking stellen en verstrekken van politiegegevens .....</b>	<b>6</b>
<b>10. Het melden van datalekken.....</b>	<b>6</b>

## Definities

In het privacybeleid Wet politiegegevens worden de volgende definities gehanteerd:

- **Algemene Verordening Gegevensbescherming (AVG)**

De Algemene Verordening Gegevensbescherming (EU 2016/679 van het Europees Parlement en de Raad van 27 april 2016. EU-wet betreffende de bescherming van natuurlijke personen, in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. Voor Nederland zijn enkele onderwerpen uitgewerkt in de Uitvoeringswet AVG (UAVG). Privacy-voorschriften zijn verder te vinden in sectorspecifieke wetgeving.

- **Wet politiegegevens (Wpg)**

De wet politiegegevens is een Nederlandse wet die de rechten en de plichten van de politie zelf, maar ook die van de burger regelt, voor wat betreft het verwerken van politiegegevens. Politiegegevens zijn persoonsgegevens die in het kader van de politietaak worden verwerkt. Naast de politie moeten ook andere organisaties zich aan de Wpg houden zoals de bijzondere opsporingsdiensten (BOD) en de buitengewoon opsporingsambtenaren (boa's).

- **Betrokkene(n)**

De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de persoonsgegevens worden verwerkt. Dit kan gaan om een inwoner, ondernemer, ambtenaar of contactpersoon van een (keten)partner.

- **Persoonsgegevens**

Informatie uit data die direct of indirect betrekking heeft op een levend persoon. Denk hierbij aan naam, adres en geboortedatum. Naast deze "gewone" persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Deze gegevens gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeur of gezondheid.

- **Verwerking**

Alles wat je met persoonsgegevens kan doen; "het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen en vernietigen

- **Functionaris Gegevensbescherming (FG)**

Een onafhankelijke en deskundige interne toezichthouder en adviseur met wettelijke taken en bevoegdheden. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van alle privacy wet- en regelgeving waaronder de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg).

## 1. Inleiding

In het privacybeleidskader heeft de gemeente Bernheze het algemene kader geformuleerd wat als kapstok fungeert voor onderliggende (beleids)documenten. Dit privacybeleid kan aangemerkt worden als een onderliggend document. Het bouwt dus verder op het algemene privacybeleidskader. Het algemene kader is vooral toegespitst op de Algemene Verordening Gegevensbescherming (AVG). De verwerking van persoonsgegevens door buitengewoon opsporingsambtenaren (boa's) valt niet alleen onder de AVG maar ook onder de Wet politiegegevens (Wpg). Daarnaast is een aantal andere regelingen van toepassing op de verwerking van politiegegevens, zoals: het Besluit politiegegevens (Bpg), het Besluit politiegegevens buitengewoon opsporingsambtenaren en de Regeling periodieke audit politiegegevens. In dit beleid worden de concrete eisen en verschillen die betrekking hebben op de Wpg verder geconcretiseerd.

## 2. Doel

Het privacybeleid van de gemeente beschrijft op welke wijze de gemeente invulling geeft aan haar verplichtingen op het gebied van de relevante privacywetgeving. Het doel van dit beleid is:

- Inzicht geven op welke wijze de gemeente Bernheze omgaat met de verwerking van persoonsgegevens onder de Wpg;
- De verwerking van persoonsgegevens onder de Wpg stroomlijnen met verwerking van persoonsgegevens onder de AVG;
- Zorgen voor een adequate procedure voor de rechten van betrokkenen onder de Wpg.

## 3. Scope

De boa's van de gemeente Bernheze kunnen naast hun opsporingstaken ook bestuursrechtelijke toezichts- en handhavingstaken hebben. Zij krijgen dan bij het verwerken van persoonsgegevens te maken met zowel de AVG als met de Wpg. De Wpg stelt andere eisen aan de verwerking van persoonsgegevens dan de AVG. Zo geldt onder andere de plicht tot delen met ieder andere opsporingsambtenaar die deze gegevens nodig heeft voor zijn werk. Dit beleid is van toepassing op de verwerking van persoonsgegevens onder de Wpg. Voor verwerking onder de AVG wordt verwezen naar het algemene privacybeleid.

## 4. Verplichtingen uit de Wpg

Zoals reeds benoemd verschilt de Wpg van de AVG. De Wpg heeft dus enkele aanvullende eisen wanneer het de verwerking van persoonsgegevens betreft. De gemeente heeft de volgende vereisten ingevoerd in haar organisatie en binnen de relevante applicaties/systemen:

- Er wordt een scheiding aangebracht tussen gegevens die op feiten zijn gebaseerd en feiten die op een persoonlijk oordeel zijn gebaseerd. (art. 4 Wpg)
- Er wordt onderscheid worden gemaakt tussen betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden. (art. 6b Wpg)
- Er vindt logging plaats in geautomatiseerde systemen van de invoer van gegevens in systemen en op termijn ook van het verzamelen, wijzigen, raadplegen, verstrekken (o.a. in de vorm van doorgifte), combineren of vernietigen van politiegegevens. (art. 32a Wpg)
- De beveiligingseisen uit het Besluit politiegegevens zijn verwerkt in het informatiebeveiligingsbeleid van de gemeente.

- Er is een verwerkingsregister dat toeziet op de verwerkingen binnen Wpg-gebied. (art. 31d Wpg)
- Er is een procedure in werking die toeziet op de planning en uitvoering van audits. (art. 33 Wpg)

## 5. Informatiebeveiliging

De gemeente heeft een informatiebeveiligingsbeleid vastgesteld wat invulling geeft aan de wettelijke beveiligingseisen op het gebied van privacy en informatiebeveiliging. Het informatiebeveiligingsbeleid voldoet aan de eisen zoals die zijn vastgelegd in de Baseline Informatiebeveiliging Overheid (BIO). Het informatiebeveiligingsbeleid geldt voor alle activiteiten van de gemeente. Ook voor de activiteiten die vallen onder de Wpg geldt dat passende technische en organisatorische maatregelen zijn genomen en geïmplementeerd. Deze maatregelen worden bovendien periodiek geëvalueerd en zo nodig geactualiseerd.

## 6. Functionaris gegevensbescherming

Net als de AVG verplicht artikel 36 van de Wpg tot het aanstellen van de FG. Een FG voor de Wpg is een onafhankelijke deskundige op het gebied van gegevensbescherming die adviseert, informeert en toezicht houdt op de naleving van Wpg. De FG wordt door de gemeente Bernheze tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van politiegegevens. De FG brengt jaarlijks een verslag uit aan het bestuur over werkzaamheden, bevindingen en aanbevelingen

## 7. Rechten van betrokkenen

De rechten van betrokkenen onder de AVG staan beschreven in het algemene privacybeleid van de gemeente. Op hoofdlijnen kunnen betrokkenen dezelfde rechten uitoefenen onder de AVG en de WPG. Er zijn echter specifieke verschillen tussen de beide regelingen. Op grond van art. 27 en 28 Wpg geldt daarom het volgende:

Een verzoek om inzage, rectificatie of vernietiging wordt afgewezen voor zover dit noodzakelijk en evenredig is:

- ter vermindering van belemmering van de gerechtelijke onderzoeken of procedures,
- ter vermindering van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen,
- ter bescherming van de openbare veiligheid, ter bescherming van de rechten en vrijheden van derden,
- ter bescherming van de nationale veiligheid en ingeval van een kennelijk ongegrond of buitensporig verzoek.

Voor de wijze waarop betrokkenen hun rechten kunnen uitoefenen en de te volgen procedure wordt verwezen naar het protocol rechten van betrokkenen.

## 8. Het bewaren, verwijderen en vernietigen van politiegegevens

Politiegegevens mogen niet oneindig lang bewaard worden. Op grond van de AVG en de Wpg dient altijd een maximale termijn gehanteerd te worden. Dit kan een specifieke termijn zijn (5 jaar) of tot het moment dat het bewaren van de gegevens niet meer noodzakelijk is voor het doel waarvoor de gegevens verkregen zijn. De Wpg hanteert een termijn van 5 jaar waarbinnen de gegevens bewaard mogen worden. Hierna dienen zij te worden verwijderd.

Het verwijderen van de gegevens betekent niet dat de gegevens definitief verwijderd zijn. De gegevens worden dan nog bewaard voor bijvoorbeeld de afhandeling van klachten en verantwoording voor het politie handelen. Zij zijn echter niet beschikbaar in het kader van ‘gewone’ opsporingstaken. Wanneer de gegevens dan voor deze beperkte gronden niet meer noodzakelijk zijn worden deze definitief verwijderd. De uiterlijke vernietigingstermijn is 5 jaar.

De Wpg maakt onderscheid tussen gegevens verzameld op grond van art. 8, 9 en 13 Wpg. De verschillende artikelen brengen verschillende bewaartermijnen en vernietigingsgronden met zich mee. De gemeente Bernheze heeft ervoor gezorgd dat deze verschillen in haar systemen zijn doorgevoerd.

## 9. Het ter beschikking stellen en verstrekken van politiegegevens

De Wpg onderscheidt het ter beschikking stellen van politiegegevens en het verstrekken ervan. Het ter beschikking stellen van politiegegevens houdt in dat deze in principe worden gedeeld met iedereen (politieagent/Boa) die de gegevens nodig heeft voor de uitoefening van zijn taak. Bij dit ‘need to know’-principe wordt altijd een noodzakelijkheids-, proportionaliteits- en subsidiariteitsafweging te gemaakt. Het gaat om gegevensverstrekking binnen het politiedomein.

Bij het verstrekken van politiegegevens gaat het om het delen van gegevens buiten het Wpg-domein. In dat geval is geborgd dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wpg en het Bpg zijn genoemd. Geborgd moet ook zijn dat wanneer gegevens verstrekt worden, er wordt voldaan aan de documentatieplicht en dat de verstrekking alleen plaatsvindt in overeenstemming met het bevoegd gezag indien dit vereist is in de wet. Het gaat dan bijvoorbeeld om verstrekkingen aan de burgemeester, een toezichthouder, een advocaat of een functionaris in het kader van de Wet bibob.

## 10. Datalekken

De datalekprocedure onder de AVG staat beschreven in het privacybeleid en datalekprotocol van de gemeente Bernheze. Hierbij geldt wederom dat de procedures inzake datalekken onder de AVG en de Wpg op grote delen overeenkomen. Er is echter een significant verschil. De mededeling van het datalek kan achterwege gelaten worden in bepaalde gevallen:

De melding van een datalek aan de betrokkene kan uitblijven voor zover dit noodzakelijk en evenredig is:

- ter vermindering van belemmering van de gerechtelijke onderzoeken of procedures,
- ter vermindering van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen,
- ter bescherming van de openbare veiligheid, ter bescherming van de rechten en vrijheden van derden,

- ter bescherming van de nationale veiligheid en ingeval van een kennelijk ongegrond of buitensporig verzoek.