Gemeente Kaag en Braassem

# GEMEENTEBLAD

Officiële uitgave van de gemeente Kaag en Braassem

Nr. 275069

24 juni

2024

## Addendum privacybeleid Wet Politiegegevens (Wpg) gemeente Kaag en Braassem

### Inleiding

Vanaf 25 mei 2018 geldt de Algemene Verordening Gegevensbescherming (AVG). De gemeente Kaag en Braassem heeft in haar privacybeleid en informatiebeveiligingsbeleid vastgelegd hoe zij omgaat met de bescherming van persoonsgegevens.

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. Deze wetten en regelgevingen kennen op enkele gebieden wat onderlinge verschillen.

Zo kent de Wpg bijvoorbeeld specifieke bewaartermijnen voor de opslag van politiegegevens, terwijl de AVG geen concrete bewaartermijnen voorschrijft. Ook stelt de Wpg andere eisen bij het delen van politiegegevens tussen verschillende partijen, is er een verplichting tot logging en zijn er in de Wpg aanvullende beperkingen en uitzonderingen op de in de AVG geldende privacyrechten van betrokkenen. Andere verplichtingen zijn vergelijkbaar maar kennen verschillen in de concrete uitwerking, zoals de verplichting voor de verwerkingsverantwoordelijke om passende technische en organisatorische maatregelen te treffen ter bescherming en beveiliging van de gegevens. In het kader van de Wpg is bijvoorbeeld ook eens per 4 jaar een externe audit verplicht en moeten elk jaar interne audits worden gehouden.

Het huidige privacybeleid van de gemeente Kaag en Braassem gaat alleen uit van de AVG. Het is daarom wenselijk er de verplichtingen uit de Wpg aan toe te voegen.

### Doelstellingen van het privacybeleid

Het privacybeleid van de gemeente Kaag en Braassem beschrijft hoe we verantwoordelijk en binnen wettelijke kaders met persoonsgegevens omgaan. Voor de reikwijdte van dit addendum bestaat het wettelijk kader voor bescherming van persoonsgegevens uit de Wpg en de genoemde regelingen. De gemeente Kaag en Braassem wil met dit addendum op het privacybeleid onder andere bereiken dat de boa's:

- Zich ten volle bewust zijn van de noodzaak om zorgvuldig en op rechtmatige wijze om te gaan met politiegegevens;
- De rechten van betrokkenen respecteren en werken volgens de vastgestelde procedures;
- Het vertrouwen van betrokkenen in de overheid niet beschamen;
- Gedrag vertonen dat past bij goed werknemerschap;
- De kans op financiële en imagoschade minimaliseren.

### De boa’s bij de gemeente Kaag en Braassem

De Gemeente Kaag en Braassem heeft verschillende werknemers in dienst, waaronder een aantal buitengewoon opsporingsambtenaren (boa’s). Boa’s zijn belast met een breed pakket aan toezichts- en handhavingstaken; zo houden ze toezicht en handhaven ze de regels om overlast en (kleine) ergernissen in de openbare ruimte tegen te gaan. Als boa’s in de uitvoering hiervan strafbare feiten constateren, verwerken zij persoonsgegevens in het kader van de opsporing en strafrechtelijke handhaving (domein I: Openbare Ruimte). Bijvoorbeeld bij het controleren van een identiteitsbewijs of bij het opleggen van een boete. Deze gegevens worden verwerkt in de applicatie CityControl.

### Wpg kader

Het normenkader van de Wpg is grotendeels gelijkluidend aan dat van de AVG. Op hoofdlijnen geldt aanvullend nog het volgende:

- De boa's van de gemeente Kaag en Braassem kunnen naast hun opsporingstaken ook bestuursrechtelijke toezichts- en handhavingstaken hebben. Zij krijgen dan bij het verwerken van persoonsgegevens te maken zowel met de AVG te maken als met de Wpg;
- In de verwerking van gegevens moet duidelijk zijn welke gegevens er worden verwerkt onder de AVG en welke onder 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.

De hierna genoemde verplichtingen uit de Wpg zijn veelal geborgd binnen onze applicatie:
- Er moet een scheiding worden aangebracht tussen gegevens die op feiten zijn gebaseerd en feiten die op een persoonlijk oordeel zijn gebaseerd;
- Er moet onderscheid worden gemaakt tussen betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden;
- Documentatie is vereist van de doelen van onderzoeken, verstrekking of doorgifte, afwijzing van verzoeken om inzage, inbreuk op de beveiliging, doorgifte buiten de EU met datum en tijd, ontvanger, redenen en doorgegeven gegevens en melding van gemeenschappelijke verwerkingen aan de Autoriteit Persoonsgegevens (AP);
- 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;
- Er worden specifieke eisen gesteld aan de informatiebeveiliging uit het Bpg;
- Er wordt een verwerkersovereenkomst afgesloten met de leverancier waarin afspraken staan opgenomen over informatiebeveiliging, datalekken en geheimhouding. De verwerkersovereenkomst dient als een Third Party Memorandum (TPM), conform de NOREA handreiking privacy audit Wpg voor boa's.

Er geldt met ingang van 2021 een verplichting tot het uitvoeren van een externe privacyaudits. De rapportage die hieruit voortvloeit moet worden verstrekt aan de AP. Als er tekortkomingen zijn geconstateerd moet 3 maanden na het uitvoeren van de audit een verbeterrapport worden opgesteld, waarop binnen een jaar een hercontrole plaatsvindt. De hercontrole geldt alleen voor die onderdelen van de wet waar de tekortkomingen geconstateerd worden. De resultaten van de hercontrole worden vastgelegd in een rapportage en eveneens verstrekt aan de AP, uiterlijk 1 jaar na het uitvoeren van de externe audit. De gemeente hanteert als raamwerk voor beheersmaatregelen (Control Framework) het door Wpg-auditoren gehanteerde raamwerk, zoals dat is opgenomen in bijlage 3 en 4 van de NOREA handreiking privacy audit Wpg voor boa's.

**Register van verwerkingen**
Net als de AVG verplicht de Wpg tot het bijhouden van een register van verwerkingen. Wel zijn er enkele verschillen die hierna met een (*) zijn aangeduid. Het register van verwerkingen in het kader van de Wpg moet het volgende bevatten:
- De naam en de contactgegevens van de verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de functionaris voor gegevensbescherming;
- De doelen van de verwerking;
- De categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties;
- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- In voorkomend geval: het gebruik van profilering. (*)
- In voorkomend geval: de categorieën van doorgiften van politiegegevens aan een derde land of een internationale organisatie.
- Een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de politiegegevens bedoeld zijn. (*)
- Zo mogelijk: de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd.
- Zo mogelijk: een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging.
- De toekenning van de autorisaties. (*)

**Informatiebeveiligingsbeleid**
Het informatiebeveiligingsbeleid is een richtinggevend en kaderstellend beleidsdocument. De gemeente Kaag en Braassem vult het aan met beleid voor informatiebeveiliging op tactisch en operationeel niveau met specifieke (beleids-) documenten.

Het informatiebeveiligingsbeleid geldt voor alle activiteiten van de gemeente Kaag en Braassem. Ook voor de activiteiten die vallen onder de Wpg geldt dat passende technische en organisatorische maatregelen moeten zijn genomen en geïmplementeerd, op basis van een risicoanalyse waaruit het risiconiveau blijkt met betrekking tot ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging. Deze maatregelen moeten bovendien periodiek worden geëvalueerd en zo nodig geactualiseerd.
De toegangsbeveiliging is zodanig ingericht dat alleen Boa's en geautoriseerden toegang hebben tot politiegegevens. Bij de verzending van politiegegevens worden deze altijd versleuteld verstuurd.

### Functionaris Gegevensbescherming
Net als de AVG verplicht artikel 36 van de Wpg tot het aanstellen van de Functionaris Gegevensbescherming (FG). Het is mogelijk dat meerdere organisaties samen één FG aanwijzen. De FG wordt door de verwerkingsverantwoordelijke tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van politiegegevens. De FG stelt jaarlijks een verslag op van zijn bevindingen en stelt het ter beschikking aan de verwerkingsverantwoordelijke.

### Rechten van betrokkenen
De rechten van betrokkenen onder de AVG staan uitgebreid beschreven in het privacybeleid van de gemeente Kaag en Braassem. Op hoofdlijnen zijn deze rechten op grond van de Wpg gelijkluidend. Specifiek voor de Wpg is er een addendum opgesteld.

### Het bewaren van politiegegevens
Politiegegevens worden niet langer bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. Politiegegevens dienen na verwijdering nog maximaal vijf jaar worden bewaard. Daarna, of binnen deze periode van vijf jaar (afhankelijk van welke bewaartermijn geldt) dient definitieve vernietiging plaats te vinden. Indien van cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens. Er wordt dan aan de bewaareisen als genoemd in de Archiefwet voldaan.
De gemeente Kaag en Braassem verwerkt politiegegevens op basis van Artikel 8 van de Wpg (uitvoering van de dagelijkse politietaak) en op basis van de artikelen over ter beschikking stellen en verstrekking van politiegegevens (Art 15-21 en 23-24). Wij verwerken geen gegevens op basis van Artikel 7a, 9, 11, 13 of 17a Wpg.
Voor alle politiegegevens is de bewaartermijn conform de wettelijke bepaling geconfigureerd, zodat geborgd wordt dat deze politiegegevens niet langer worden bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt.
Daarnaast voert de gemeente voor elke verwerking van politiegegevens een Data Protection Impact Assessment (DPIA) uit, die elke 3 jaar deze wordt herzien. Daarin worden de volgende principes getoetst en geborgd:
- Gegevensbescherming door beveiliging en ontwerp;
- Gegevensbescherming door standaard-instellingen.

### Het ter beschikking stellen en verstrekken van politiegegevens
De Wpg maakt een onderscheid tussen 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 eenieder die de gegevens nodig heeft voor de uitoefening van zijn taak. Bij dit ‘need to know’-principe dient altijd een noodzakelijkheids-, proportionaliteits- en subsidiariteitsafweging te worden gemaakt. Het ter beschikking stellen voltrekt zich dus binnen het Wpg-domein.
Bij het verstrekken van politiegegevens gaat het om het delen van gegevens buiten het Wpg-domein. In dat geval moet zijn 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.

### Het melden van datalekken
De datalek procedure onder de AVG staan uitgebreid beschreven in het privacybeleid van de gemeente Kaag en Braassem. Op hoofdlijnen zijn deze rechten op grond van de Wpg gelijkluidend. Specifiek voor de Wpg geldt nog het volgende:
- Op deze mededelingsplicht zijn enkele uitzonderingen van toepassing, onder andere als de mededeling achterwege moet blijven ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures en ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

### Bewustwording
Het zorgvuldig omgaan met persoonsgegevens is enerzijds een kwestie van het organiseren van een goede informatieveiligheid en het zorgvuldig inrichten van werkprocessen, anderzijds is het een zaak van bewustwording bij de boa's. Het bewustzijn wordt voortdurend aangescherpt, zodat kennis van risico’s wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.

Elke nieuwe medewerker moet daarom verplicht een Wpg training doorlopen. Daarvan wordt een notitie vastgelegd in het personeelsdossier. Boa's die al in dienst zijn en deze training nog niet hebben doorlopen, doorlopen deze training alsnog. Daarnaast is er in ieder geval jaarlijks aanvullend aandacht voor bewustwording rondom de omgang met politiegegevens. Dit kan bijvoorbeeld in de vorm van een aanvullende training, een bijeenkomst over een specifiek Wpg-onderwerp of in de vorm van een toets. Ook van deelname aan deze initiatieven wordt een notitie in het personeelsdossier gemaakt.

**Open communicatie**
Betrokkenen moeten erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden verwerkt. De gemeente Kaag en Braassem creëert dat vertrouwen door inzichtelijk te maken, door middel van verschillende communicatiekanalen, op welke wijze zij persoonsgegevens verwerkt en beheert. Dit staat in de privacyverklaring die op de website is te vinden.

*Aldus vastgesteld door het college van burgemeester en wethouders van de gemeente Kaag en Braassem op 28 mei 2024,*
*de secretaris,*
*J.J. Démoed*

*de burgemeester,*
*A. Heijstee-Bolt*