gemeente Tiel

GEMEENTEBLAD

Officiële uitgave van de gemeente Tiel

Nr. 5017

2 januari

2024

Addendum privacybeleid gemeente Tiel Beleid Wet politiegegevens

Inleiding

Sinds 25 mei 2018 geldt de Algemene Verordening Gegevensbescherming (AVG). Om invulling te geven aan deze wetgeving heeft de gemeente Tiel in haar privacybeleid (Privacybeleid Gemeente Tiel 2023-2025) en informatiebeveiligingsbeleid vastgelegd hoe zij omgaat met de bescherming van persoonsgegevens.

Buitengewoon opsporingsambtenaren (boa's) hebben naast de AVG te maken met de Wet politiegegevens (Wpg). Boa's zijn ambtenaren met een specifieke opsporingsbevoegdheid. Wanneer boa's persoonsgegevens verwerken in het kader hun opsporingstaken, is hierop de Wpg van toepassing. De persoonsgegevens die zij voor hun opsporingstaak verwerken worden politiegegevens genoemd. In de Wpg worden eisen gesteld aan de verwerking van politiegegevens om de privacy van betrokkenen te waarborgen en om misbruik tegen te gaan. Naast de Wpg is een aantal andere regelingen van toepassing op de verwerking van politiegegevens, zoals het Besluit politiegegevens (Bpg), het Besluit politiegegevens buitengewoon opsporingsambtenaren (BpgBoa) en de Regeling periodieke audit politiegegevens.

De AVG en de Wpg bestaan naast elkaar, maar kennen op een aantal punten overlap. Net als onder de AVG gelden voor de verwerking van politiegegevens de beginselen van doelbinding, noodzakelijkheid, rechtmatigheid en juistheid. Daarnaast verplicht ook de Wpg tot het treffen van beveiligingsmaatregelen, het bijhouden van een register, het afsluiten van verwerkersovereenkomsten, het melden van datalekken, het voorzien in de rechten van betrokkenen, het aanstellen van een Functionaris Gegevensbescherming (FG) en het uitvoeren van Data Protection Impact Assessments (DPIA's). Op andere onderdelen is er sprake van verschillen tussen de AVG en Wpg. 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 (vastlegging langs elektronische weg) en zijn er in de Wpg aanvullende beperkingen en uitzonderingen op de in de AVG geldende privacyrechten van betrokkenen. De Wpg kent tot slot een auditverplichting.

Het algemene privacybeleid van Tiel beschrijft hoe de gemeente invulling geeft aan de verplichtingen uit de AVG. Dit addendum bij het algemene privacybeleid beschrijft een aantal verplichtingen die op grond van de Wpg specifiek gelden voor de verwerking van politiegegevens. Op de normen uit de Wpg die overeenkomen met die van de AVG is het algemene privacybeleid van overeenkomstige toepassing.

Boa's in de gemeente Tiel

Boa's hebben zowel toezichthoudende taken als opsporingstaken. De verwerking van persoonsgegevens met betrekking tot de toezichthoudende taak valt onder de AVG. Op de verwerking van persoonsgegevens in het kader van de uitvoering van hun opsporingstaken is de Wpg van toepassing. Het gaat om de opsporing van strafbare feiten die in een akte van opsporingsbevoegdheid of in een aanwijzing zijn opgelegd aan de boa. De werkgever van de boa wordt op grond van het BpgBoa als verwerkingsverantwoordelijke aangemerkt voor de verwerking van politiegegevens.

De gemeente Tiel heeft alleen boa's in dienst die werkzaam zijn in het domein Onderwijs[1]. Deze boa's zijn belast met de opsporing van strafbare feiten op grond van (onder meer) de Leerplichtwet. Voor hun opsporingstaak verwerken de boa's politiegegevens in een informatiesysteem, doen zij onderzoek naar mogelijk ongeoorloofd verzuim, leggen zij huisbezoeken af, voeren ze gesprekken met betrokkenen en kunnen zij een proces-verbaal opmaken.

De boa's van de gemeente Tiel verwerken uitsluitend politiegegevens op grond van artikel 8 Wpg (uitvoering van de dagelijkse politietaak).

Doelstellingen van het beleid Wet politiegegevens

Het privacybeleid van de gemeente beschrijft op welke wijze binnen de wettelijke kaders met persoonsgegevens wordt omgegaan. Voor de reikwijdte van dit addendum bestaat het wettelijk kader voor bescherming van persoonsgegevens uit de Wpg en de genoemde regelingen. De gemeente Tiel wil met dit addendum op het privacybeleid onder andere bereiken dat de boa's:

1) Zie Regeling domeinlijsten buitengewoon opsporingsambtenaar

- 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

Wpg-kader

Het normenkader van de Wpg is grotendeels gelijkluidend aan dat van de AVG. Toch zijn er ook belangrijke verschillen tussen het verwerken van persoonsgegevens onder de AVG en het verwerken van politiegegevens onder de Wpg.

De boa's van de gemeente kunnen naast hun opsporingstaken ook bestuursrechtelijke toezichts- en handhavingstaken hebben. Zij krijgen dan bij het verwerken van persoonsgegevens zowel met de AVG als met de Wpg te maken.

Om onrechtmatige gegevensverwerking te voorkomen is het van belang dat het duidelijk is welke gegevens er worden verwerkt onder de AVG en welke onder de Wpg. Soms gelden onder de Wpg namelijk strengere, dan wel andere, regels. Zo zijn boa's bij de verstrekking van politiegegevens gehouden aan het zogeheten gesloten verstrekkingsregime van de Wpg en moeten persoonsgegevens onder het Wpg-regime worden gedeeld met iedere andere opsporingsambtenaar die deze gegevens nodig heeft voor zijn taak.

De hierna genoemde verplichtingen uit de Wpg en het Bpg zijn geborgd binnen het informatiesysteem waarin politiegegevens worden verwerkt:

- Er moet onderscheid worden aangebracht tussen gegevens die op feiten zijn gebaseerd en gegevens die op een persoonlijk oordeel zijn gebaseerd
- Er moet onderscheid worden gemaakt tussen betrokkenen, zoals verdachten, slachtoffers, getuigen en overige derden en veroordeelden
- Er wordt documentatie bijgehouden van de doelen van onderzoeken, verstrekking of doorgifte
- Er vindt logging plaats in geautomatiseerde systemen van de invoer van gegevens en op termijn ook van het verzamelen, wijzigen, raadplegen, verstrekken (o.a. in de vorm van doorgifte), combineren of vernietigen van politiegegevens

Op grond van de Wpg is de gemeente verplicht om de naleving van de wet periodiek te toetsen door middel van audits[2]. Hiertoe laat de gemeente eens per vier jaar een externe privacy audit uitvoeren door een onafhankelijke auditor. Daarnaast wordt de naleving van de Wpg ieder jaar getoetst door middel van een interne audit. De privacy audit heeft tot doel om op systematische wijze te toetsen of aan de bepalingen van de wet op adequate wijze uitvoering is gegeven. De rapportage die hieruit voortvloeit moet worden verstrekt aan de Autoriteit Persoonsgegevens (AP). Als er tekortkomingen zijn geconstateerd moet binnen drie 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 één jaar na het uitvoeren van de externe audit.

Register van verwerkingen

Net als onder de AVG is de verwerkingsverantwoordelijke onder de Wpg verplicht om een register van verwerkingen bij te houden. In het verwerkingsregister staat onder meer welke persoonsgegevens worden verwerkt, met welk doel dat gebeurt, aan wie deze eventueel worden verstrekt en hoe lang de gegevens bewaard blijven. Afwijkend ten opzichte van de AVG is dat het register van verwerkingen in het kader van de Wpg de volgende gegevens moet bevatten:

- In voorkomend geval: het gebruik van profilering
- Een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de politiegegevens bedoeld zijn
- Aan wie autorisaties zijn toegekend voor het verwerken van politiegegevens

Informatiebeveiligingsbeleid

In het informatiebeveiligingsbeleid van de gemeente zijn maatregelen genoemd om (persoons)gegevens te beschermen. Deze maatregelen dienen om misbruik, verlies, onbevoegde toegang en andere onge-

2) Zie artikel 33 Wpg, artikel 6:5. Besluit politiegegevens en Regeling periodieke audit politiegegevens.

wenste handelingen met (persoons)gegevens tegen te gaan. Het informatiebeveiligingsbeleid is ook van toepassing op de verwerking van politiegegevens.

Voor het Wpg-informatiesysteem is een specifiek autorisatiebeleid vastgesteld. In het beleid is uitgewerkt hoe en onder welke voorwaarden toegang tot het informatiesysteem en de daarin opgeslagen politiegegevens wordt verleend en op welke wijze de gemeente controleert of de procedure correct wordt uitgevoerd.

Functionaris Gegevensbescherming
Net als de AVG verplicht de Wpg de verwerkingsverantwoordelijke tot het aanstellen van een FG. De FG houdt (onder meer) toezicht op de naleving van de Wpg en het gemeentelijk beleid voor de verwerking van politiegegevens. 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 beschreven in het privacybeleid van de gemeente. Op hoofdlijnen zijn deze rechten op grond van de Wpg gelijkluidend. Specifiek voor de Wpg geldt nog het volgende:

Een verzoek om inzage, rectificatie of vernietiging wordt afgewezen voor zover dit noodzakelijk en evenredig is:
- Ter vermijding van belemmering van gerechtelijke onderzoeken of procedures
- Ter vermijding 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
- In geval van een kennelijk ongegrond of buitensporig verzoek, als bedoeld in artikel 24a lid 4 Wpg

Een gehele of gedeeltelijke afwijzing van een verzoek is schriftelijk en bevat de redenen voor de afwijzing.

Het bewaren van politiegegevens
Politiegegevens worden niet langer bewaard dan strikt noodzakelijk is voor de uitvoering van de aan de boa opgedragen opsporingstaak of dan is toegestaan op grond van de wet.

De gemeente zorgt ervoor dat politiegegevens voor de uitvoering van de opsporingstaak zoals bedoeld in artikel 8 Wpg:
- Gedurende een jaar beschikbaar zijn in het kader van de uitvoering van de opsporingstaak
- Na een jaar slechts beschikbaar zijn voor gericht zoeken
- Na vijf jaar worden verwijderd; de gegeven worden dan alleen voor audits en klachten gebruikt
- Na tien jaar worden vernietigd

Het ter beschikking stellen en verstrekken van politiegegevens
De Wpg maakt een onderscheid tussen het ter beschikking stellen van politiegegevens en het verstrekken ervan. De gemeente stelt politiegegevens conform de wet ter beschikking op basis van het ‘free flow of information’ principe, indien het ter beschikking stellen van politiegegevens noodzakelijk is voor de uitoefening van de taken binnen het Wpg-domein. Hierbij dient altijd een noodzakelijkheids-, proportionaliteits- en subsidiariteitsafweging te worden gemaakt.

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 genoemd in de Wpg en het Bpg en voor zover dit mogelijk is op basis van een wettelijke bepaling in de Wpg en het Bpg. De ontvanger van de politiegegevens is vervolgens onderworpen aan de geheimhoudingsplicht uit de Wpg. De gemeente legt verstrekkingen van politiegegevens vast en voldoet daarmee aan de documentatieplicht die geldt op grond van de Wpg.

De regels omtrent het ter beschikking stellen en verstrekken van politiegegevens zijn verder uitgewerkt in de werkinstructie voor de leerplicht boa’s.

Het melden van datalekken
De datalekprocedure onder de AVG staat beschreven in het privacybeleid van de gemeente Tiel. Op hoofdlijnen komt deze overeen met de procedure onder de Wpg. Specifiek voor de Wpg geldt nog het volgende:

De mededeling aan betrokkene kan worden uitgesteld, beperkt of achterwege gelaten op de gronden zoals vermeld in artikel 27 Wpg. Bijvoorbeeld wanneer het achterwege laten van een dergelijke mededeling noodzakelijk is ter vermijding van belemmering van gerechtelijke onderzoeken of procedures.

Bewustwording
Naast het vaststellen van beleid en het treffen van passende beveiligingsmaatregelen is zorgvuldig omgaan met persoonsgegevens ook een kwestie van bewustwording. Het privacy bewustzijn van de boa's wordt voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.

Medewerkers moeten verplicht trainingen doorlopen op het gebied van privacy en informatiebeveiliging. Daarnaast is een werkinstructie opgesteld voor de leerplicht boa's waarin is uitgewerkt hoe en onder welke voorwaarden politiegegevens mogen worden verwerkt.

Transparantie
De gemeente Tiel vindt een zorgvuldige verwerking van persoonsgegevens belangrijk. Hoe de gemeente omgaat met persoonsgegevens en welke rechten betrokkenen hebben wordt inzichtelijk gemaakt in de privacyverklaring die op de website is te vinden.