gemeente Neder-Betuwe

GEMEENTEBLAD

Officiële uitgave van de gemeente Neder-Betuwe

Nr. 43067

29 januari 2024

Addendum privacybeleid Wpg gemeente Neder-Betuwe behorende bij het Privacybeleid gemeente Neder-Betuwe vastgesteld d.d. 30 april 2019

Burgemeester en wethouders van de gemeente Neder-Betuwe

Overwegende dat de gemeente Neder-Betuwe middels beleid privacy wenst te waarborgen

Gelet op de Wet politiegegevens

Besluit vast te stellen het:

Addendum privacybeleid Wpg gemeente Neder-Betuwe behorende bij het Privacybeleid gemeente Neder-Betuwe vastgesteld d.d. 30 april 2019.

De Wet politiegegevens vs. de Algemene Verordening Gegevensbescherming
Het normenkader van de Wet politiegegevens (verder: Wpg) is grotendeels gelijkluidend aan dat van de AVG. Op hoofdlijnen geldt aanvullend nog het volgende:

- De betrokken medewerkers van de gemeente kunnen naast hun (betrokkenheid bij) opsporingstaken ook bestuursrechtelijke toezichts- en handhavingstaken hebben. Zij krijgen dan bij het verwerken van persoonsgegevens te maken zowel met de AVG 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.

Verplichtingen uit de Wet politiegegevens
Er zijn een aantal verplichtingen die voortkomen uit de Wpg en die reeds zijn of worden geborgd in onze systemen en applicaties:

- 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 Besluit politiegegevens (Bpg).

Ook binnen de Wpg dient er een register van verwerkingen te zijn. Daarop aanvullend wordt vormgegeven aan expliciet in de Wpg opgenomen aspecten (indien van toepassing profilering, aanwijzing rechtsgrondslag verwerking en toekennen autorisaties).

De Functionaris Gegevensbescherming (FG)
Net als de AVG verplicht artikel 36 van de Wpg tot het aanstellen van de 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.
Daarnaast voorziet de Wpg in het aanwijzen van een bevoegd functionaris met enkele specifieke taken (autoriseren, bepalen delen van gegevens, herkomst etc).

Rechten van betrokkenen
De rechten van betrokkenen onder de AVG staan uitgebreid beschreven in het privacybeleid van de gemeente. 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.

Alle politiegegevens worden gelabeld in artikel 8, 9 en 13 informatie. Voor elk label 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.

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. 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 betrokken medewerkers. Het bewustzijn wordt voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.
Elke nieuwe medewerker werkt daarom volgens het handboek en is daar over geïnstrueerd. Daarvan wordt een notitie vastgelegd in het personeelsdossier. Betrokken medewerkers die al in dienst zijn en dit handboek nog niet kende en de instructie nog niet hebben doorlopen, ontvangen en doorlopen die 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 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.