

Addendum privacybeleid Wet politiegegevens Brunssum

INLEIDING

Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht. De gemeente Brunssum heeft in haar privacy- 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 gaat alleen uit van de AVG. Dit addendum voegt de Wpg-verplichtingen toe.

DOELSTELLINGEN VAN HET PRIVACYBELEID

Het privacybeleid van de gemeente Brunssum beschrijft hoe we op een zorgvuldige, verantwoorde manier en binnen de wettelijke kaders omgaan met persoonsgegevens. Voor de reikwijdte van dit addendum bestaat het wettelijk kader voor bescherming van persoonsgegevens uit de Wpg en de genoemde regelingen. De gemeente Brunssum streeft ernaar om:

- Boa's en de organisatie zich ten volle bewust zijn van de noodzaak om zorgvuldig en op rechtmatige wijze om te gaan met politiegegevens;
- De rechten van betrokkenen worden gerespecteerd en dat er gewerkt wordt volgens de vastgestelde procedures;
- Het vertrouwen van betrokkenen in de overheid is gewaarborgd;
- Er gedrag wordt vertoond dat past bij goed werknemerschap;

WPG NORMENKADER

De Wpg biedt een normenkader dat grotendeels gelijk is aan dat van de AVG, met een aantal belangrijke aanvullingen, zoals:

- Boa's kunnen zowel opsporingstaken als bestuursrechtelijke toezichts- en handhavingstaken uitvoeren. Bij de verwerking van persoonsgegevens moeten zij zowel de bepalingen van de AVG als de Wpg naleven;
- Het moet duidelijk zijn welke gegevens onder de AVG vallen en welke onder de Wpg. De Wpg stelt andere eisen aan de verwerking van persoonsgegevens, waaronder de verplichting om politiegegevens te delen met andere opsporingsambtenaren die de gegevens nodig hebben voor hun werk.

De verplichtingen uit de Wpg die binnen de gemeente Brunssum worden geborgd zijn onder andere:

- Het maken van een scheiding tussen feitelijke gegevens en gegevens die op een persoonlijk oordeel zijn gebaseerd;
- Het onderscheiden van betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden;
- Het documenteren van de doelen van onderzoeken, de verstrekking van gegevens, verzoeken om inzage, inbreuken op de beveiliging, de doorgifte van gegevens buiten de EU, en de melding van gezamenlijke verwerkingen aan de Autoriteit Persoonsgegevens (AP);
- Logging van gegevensinvoer in systemen en het registreren van het verzamelen, wijzigen, raadplegen, verstrekken (o.a. in de vorm van doorgifte), combineren of vernietigen van politiegegevens;
- Het naleven van de eisen van het Besluit politiegegevens (Bpg) met betrekking tot informatiebeveiliging.

EXTERNE EN INTERNE AUDITS

Sinds 2021 is de gemeente Brunssum verplicht om externe privacyaudits uit te voeren, waarvan de resultaten aan de AP moeten worden verstrekt. Bij geconstateerde tekortkomingen moet binnen drie maanden een verbeterrapport worden opgesteld. Een hercontrole vindt plaats binnen een jaar na het auditrapport.

REGISTER VAN VERWERKINGEN

Net als de AVG verplicht de Wpg de gemeente Brunssum om een register van verwerkingen bij te houden, met enkele verschillen die specifiek zijn voor de Wpg. Het register bevat onder andere:

- De naam en contactgegevens van de verwerkingsverantwoordelijke en de functionaris voor gegevensbescherming;
- De doelen van de verwerking van politiegegevens;
- De categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties;
- 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.
- De rechtsgrondslag van de verwerking, met inbegrip van doorgiften;
- De beoogde bewaartermijnen van de gegevens;
- Beschrijving van de technische en organisatorische maatregelen ter beveiliging van de gegevens.

INFORMATIEBEVEILIGINGSBELEID

Het informatiebeveiligingsbeleid van de gemeente Brunssum is richtinggevend en stelt een kader voor de bescherming van gegevens. Voor de verwerkingen die vallen onder de Wpg moeten passende technische en organisatorische maatregelen worden getroffen, gebaseerd op een risicoanalyse. Deze maatregelen moeten periodiek worden geëvalueerd en aangepast waar nodig.

FUNCTIONARIS GEGEVENSBESCHERMING (FG) EN BEVOEGDE FUNCTIONARIS

Net als de AVG verplicht artikel 36 van de Wpg de gemeente Brunssum om een FG aan te stellen. De FG wordt betrokken bij alle zaken die betrekking hebben op de bescherming van politiegegevens. De FG stelt jaarlijks een verslag op van de bevindingen.

De taak van bevoegd functionaris is beschreven in artikel 2:10, eerste lid, van het Besluit politiegegevens (Bpg). Het moet een persoon zijn met voldoende kennis en vaardigheden over dit type gegevens. Deze functionaris beslist bijvoorbeeld wie er toegang mag hebben tot deze gegevens en of ze verstrekt kunnen worden aan een samenwerkingspartner. Iedere artikel 9-verwerking dient een bevoegd functionaris (BF) te hebben. De bevoegd functionaris heeft onder andere de volgende taken:

- het doel van de artikel 9-verwerking omschrijven en vastleggen;
- het autoriseren van personen voor de betreffende verwerking;
- bepalen of gegevens voor andere doeleinden mogen worden gebruikt;
- zorgen dat voor alle gegevens de herkomst en wijze van verkrijgen wordt vastgelegd;
- bewaken dat gegevensrechtmatig worden verkregen en verwerkt.

RECHTEN VAN BETROKKENEN

De rechten van betrokkenen zoals vastgelegd in de AVG, waaronder het recht op inzage, rectificatie, verwijdering en bezwaar, blijven ook van toepassing onder de Wpg. Echter, de Wpg bevat enkele aanvullende bepalingen die in bepaalde situaties de beperking van deze rechten mogelijk maken, bijvoorbeeld wanneer dit noodzakelijk is om nadelige gevolgen voor strafrechtelijke onderzoeken te voorkomen. Maar ook de volgende rechten:

- Recht van inzage (Art. 25 Wpg): Betrokkenen kunnen een verzoek indienen om inzicht te krijgen in hun politiegegevens bij de gemeente;
- Recht op rectificatie, aanvulling of vernietiging (Art. 28 Wpg): Betrokkenen kunnen verzoeken om onjuiste gegevens te corrigeren, aan te vullen of te vernietigen.

BEWAARTERMIJN

De Wpg bepaalt specifieke termijnen voor het bewaren van politiegegevens. Politiegegevens die zijn verwijderd op grond van de artikelen 8 en 9 van de Wpg, moeten gedurende vijf jaar bewaard worden om bijvoorbeeld klachten af te handelen of audits te verrichten. In sommige gevallen kunnen deze gegevens opnieuw verwerkt worden, bijvoorbeeld voor wetenschappelijk onderzoek of statistische doeleinden, maar dit kan alleen in opdracht van de Officier van Justitie.

VERSTREKKEN EN TER BESCHIKKING STELLEN 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.

DATALEKKEN

De procedure voor het melden van datalekken is in lijn met de AVG en de Wpg. Bij datalekken die betrekking hebben op politiegegevens, gelden aanvullende uitzonderingen, bijvoorbeeld wanneer de mededeling achterwege moet blijven om gerechtelijke onderzoeken of procedures niet te belemmeren, of om nadelige gevolgen voor de voorkoming, opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen te voorkomen.

BEWUSTWORDING

Het is essentieel dat boa's zich bewust zijn van het belang van zorgvuldig omgaan met politiegegevens. Alle nieuwe medewerkers moeten verplicht een training over de Wpg volgen. Ook bestaande medewerkers dienen deze training te doorlopen, en er wordt jaarlijks extra aandacht besteed aan bewustwording rondom de omgang met politiegegevens.

OPEN COMMUNICATIE

De gemeente Brunssum maakt het voor betrokkenen mogelijk om in te zien hoe hun persoonsgegevens worden verwerkt. Deze informatie wordt aangeboden via de privacyverklaring, die beschikbaar is op de gemeentelijke website van Brunssum.