

Privacybeleid Wet Politiegegevens

Gemeente Papendrecht

Vastgesteld door
College 10-12-2024
Versie 1.0

Inhoudsopgave

Inleiding	3
Doelstellingen van het privacybeleid	3
Wpg kader	4
Register van verwerkingen	4
Informatiebeveiligingsbeleid	5
FG en bevoegd functionaris	5
Rechten van betrokkenen	6
Het bewaren van politiegegevens	7
Het ter beschikking stellen van politiegegevens	9
Het melden van datalekken	9
Bewustwording	9
Open communicatie	10

Inleiding

Vanaf 25 mei 2018 geldt de Algemene Verordening Gegevensbescherming (AVG). Gemeente Papendrecht 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 boa's en de Regeling periodieke audit politiegegevens. Deze wetten en regelingen 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 verwerkings-verantwoordelijke 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 Papendrecht gaat alleen uit van de AVG. Het is daarom wenselijk ook de verplichtingen uit de Wpg in beleid vast te leggen.

Doelstellingen van het privacybeleid

Het privacybeleid van de gemeente beschrijft hoe we verantwoordelijk en binnen wettelijke kaders met persoonsgegevens omgaan. Voor de reikwijdte van dit privacybeleid bestaat het wettelijk kader voor bescherming van persoonsgegevens uit de Wpg en de genoemde regelingen. De gemeente wil met dit Wpg beleid 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.

Wpg kader

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

- De boa's van de gemeente 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 politiegegevens nodig heeft voor zijn werk. Deze plicht geldt niet voor het uitvoeren van een bestuursrechtelijke toezichtstaak.

De hierna genoemde verplichtingen uit de Wpg zijn veelal geborgd binnen het Boa Registratie Systeem (BRS), dat door de gemeente Papendrecht is aangeschaft bij de leverancier NatuurNetwerk BV.

- Er wordt een scheiding aangebracht tussen gegevens die op feiten zijn gebaseerd en feiten die op een persoonlijk oordeel zijn gebaseerd;
- Er wordt onderscheid 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 geldt met ingang van 2021 een verplichting tot het uitvoeren van een externe privacyaudits elke 4 jaar. De rapportage die hieruit voortvloeit is verstrekt aan de AP. De tekortkomingen die zijn geconstateerd zijn na het uitvoeren van de audit in een verbeterrapport opgesteld. Naar aanleiding van het verbeterplan zijn diverse maatregelen getroffen. De belangrijkste in deze was de aanschaf van het BRS. In 2025 zal weer een externe audit worden uitgevoerd.

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. (*)

De Wpg processen zijn opgenomen in het verwerkingsregister iNavigator en voor het aanbrengen mutaties hierin, bestaat een werkinstructie.

Informatiebeveiligingsbeleid

De gemeente Papendrecht heeft een eigen informatiebeveiligingsbeleid. Dit is een richtinggevend en kaderstellend beleidsdocument. De informatiebeveiliging binnen de gemeente Papendrecht vindt plaats volgens een algemeen erkende overheidsnorm (BIO).

De toereikendheid van de informatiebeveiliging blijkt uit de volgende certificering en verklaring van toepasselijkheid:

- Eigen controles of eigen mededelingen over de beveiligingsmaatregelen
- Bevindingen gedaan en beschreven ten behoeve van ENSIA 2023 en de voorlopige resultaten van ENSIA 2024
- Strategisch beleid Informatiebeveiliging Drechtsteden 20-24 (geactualiseerde versie vanaf november 2024 voor 2025-2028)
- Informatieveiligheidsplan Drechtsteden IB plan 2024

FG en bevoegd functionaris

De Functionaris Gegevensbescherming (FG)

Artikel 36 van de Wet politiegegevens (Wpg) verplicht, net als de Algemene verordening gegevensbescherming (AVG), tot het aanstellen van een Functionaris Gegevensbescherming (FG). De gemeente Papendrecht heeft een FG aangesteld die verantwoordelijk is voor de naleving van zowel de Wpg als de AVG. Deze FG is officieel aangemeld bij de Autoriteit Persoonsgegevens (AP). De FG wordt door de verwerkingsverantwoordelijke tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van politiegegevens. De FG beschrijft jaarlijks zijn bevindingen op het gebied van de Wpg in een jaarrapport.

De bevoegd functionaris in het kader van een artikel 9 Wpg verwerking.

Indien sprake is van het verwerken van politiegegevens voor de dagelijkse taak zijn de waarborgen van artikel 8 Wpg van toepassing. Indien een diepgaander onderzoek naar handhaving van de rechtsorde in een bepaald geval moet worden gedaan kan sprake zijn van een art 9 Wpg verwerking. Hiervoor gelden striktere eisen en is het verplicht een dit onder toezicht van een Bevoegd Functionaris (BF) te laten doen, die verantwoordelijk is voor het waarborgen van de rechtmatige verwerking van gegevens onder artikel 9 Wpg.

De BF moet een persoon zijn met voldoende kennis en vaardigheden met betrekking tot dit type gegevens. Om deze rol goed te kunnen vervullen, zullen de aangewezen functionarissen specifieke trainingen volgen over de verwerking van politiegegevens en de verantwoordelijkheden die daarbij horen.

De BF beslist bijvoorbeeld wie toegang mag hebben tot de gegevens en of ze mogen worden verstrekt aan een samenwerkingspartner. Daarnaast heeft de BF de volgende taken:

- het omschrijven en vastleggen van het doel van de artikel 9-verwerking;
- het autoriseren van personen voor de betreffende verwerking;
- het bepalen of gegevens voor andere doeleinden mogen worden gebruikt;
- het vastleggen van de herkomst en wijze van verkrijging van de gegevens;
- het bewaken dat gegevens rechtmatig worden verkregen en verwerkt.

In de organisatie wordt de Teamcoördinator Handhaving aangewezen als Bevoegd Functionaris. Daarnaast worden twee plaatsvervangers aangesteld om de continuïteit te waarborgen. Zij vervullen de rol van 'hoeder' van de gegevens die onder artikel 9 Wpg worden verwerkt.

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 gelijkloidend. Ten behoeve van verzoeken op grond van de Wpg wordt een digitale ingang gerealiseerd via de website van de gemeente Papendrecht.

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.

Binnen de Wpg processen, zoals opgenomen in het verwerkingsregister, wordt gebruik gemaakt van BRS van NatuurNetwerk BV. Bij gebruik van BRS worden, voor zover mogelijk, de verwerkings- en bewaartermijnen geautomatiseerd toegepast conform artikel 8, 9, en 13 Wpg. Met functionaliteit voor het vastleggen van de artikel 9-doelen en het vastleggen van verstrekkingen kan aan elementen uit de documentatieplicht worden voldaan (artikel 32 lid 1 onder a en b Wpg).

Categorie	Termijn verwerking en bewaring	Motivatie
Gegevens Boa	Variabel - Zolang de Boa gebruik maakt van BRS, of indien van toepassing, gedurende de periode van een klacht of verzetszaak.	Om gebruik te kunnen maken van BRS zijn de gegevens Boa nodig.
Gegevens overige betrokkenen	Variabel – Zolang de betrokkene geregistreerd staat bij en/of gekoppeld is aan een incident	De gegevens van betrokkene zijn noodzakelijk voor de registratie van een incident in het kader van de opsporingstaken van de Boa.
Gegevens incident – art. 8 Wpg	Variabel – - De verzamelde Politiegegevens kunnen voor de uitvoering van de dagelijkse politietaken worden verwerkt gedurende 1 jaar. - Persoonsgegevens waarvan de termijn is verstreken, kunnen geautomatiseerd worden vergeleken om verbanden vast te stellen, tot maximaal 5 jaar na eerste verwerking, waarna zij worden verwijderd. - De verwijderde Politiegegevens worden gedurende 5 jaar bewaard voor afhandeling van klachten, verantwoording van verrichtingen, en in bijzondere gevallen en na opdracht van het bevoegd gezag, voor het hernieuwd verwerken waarna zij worden vernietigd.	Artikel 8 (1), (2) en (6) jo. 14 (1) Wpg
Gegevens incident – art. 9 Wpg	Variabel – Politiegegevens kunnen worden verwerkt zolang het doel waar ze oorspronkelijk voor vastgelegd zijn, niet vervuld is. In de praktijk betekent dit: tot een veroordeling heeft plaatsgevonden of het strafbaar feit verjaard is.	Artikel 9 (2) en (4) jo. 14 (1) Wpg

	• Politiegegevens die niet langer noodzakelijk zijn voor het onderzoek kunnen nog 6 maanden bewaard blijven om te bezien of zij aanleiding geven tot een nieuwe artikel 9-verwerking. • De verwijderde Politiegegevens worden gedurende 5 jaar bewaard voor afhandeling van klachten en verantwoording van verrichtingen, en in bijzondere gevallen en na opdracht van het bevoegd gezag, voor het hernieuwd verwerken, waarna zij worden vernietigd.	
Gegevens incident – art. 13 Wpg	Variabel – Zolang verwerking is vereist en toegestaan ingevolge het betreffende art. 13 - reglement	Artikel 13 (4) Wpg
Gegevens mutatie	Onbeperkt.	Zolang het incident geregistreerd staat in BRS dient tevens inzichtelijk te blijven welke mutaties dienaangaande hebben plaatsgevonden. Na verstrijken van die periode worden de mutatiegegevens geanonimiseerd.
Logging wijziging door gebruiker	Variabel – Zolang incident 'actief' is ingevolge artikel 8, 9 of 13 Wpg, of langer in het geval van een klacht of verzetsprocedure.	De logging kan een rol spelen bij bijvoorbeeld klachten. Om die reden wordt aangesloten bij de bewaartermijn ingevolge artikel 8, 9 en 13 Wpg.
Systeem- en Errorlogging	Variabel – Zolang incident 'actief' is ingevolge artikel 8, 9 of 13 Wpg, of langer in het geval van een klacht of verzetsprocedure.	De logging kan een rol spelen bij bijvoorbeeld klachten. Om die reden wordt aangesloten bij de bewaartermijn ingevolge artikel 8, 9 en 13 Wpg.
Gebruikslogging	Variabel – Zolang incident 'actief' is ingevolge artikel 8, 9 of 13 Wpg, of langer in het geval van een klacht of verzetsprocedure.	De logging kan een rol spelen bij bijvoorbeeld klachten. Om die reden wordt aangesloten bij de bewaartermijn ingevolge artikel 8, 9 en 13 Wpg.

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.

Voor op de juiste manier gegevens ter beschikking stellen wordt aansluiting gezocht bij de Verstrekkingswijzer Wpg voor Boa's.

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 gelijklopend. Datalekken kunnen worden gemeld in het daarvoor ontworpen formulier dat op het intranet van de gemeente Papendrecht staat. Hier is tevens de mogelijkheid opgenomen tot het melden van datalekken die specifiek zien op politiegegevens. Ook voor het afhandelen van datalekken is een procesomschrijving die dan wordt gevolgd.

Op deze mededelingsplicht zijn enkele uitzonderingen van toepassing, onder andere als de mededeling achterwege moet blijven ter vermindering van belemmering van de gerechtelijke onderzoeken of procedures en ter vermindering van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen. Op deze mededelingsplicht zijn enkele uitzonderingen van toepassing, onder andere als de mededeling achterwege moet blijven ter vermindering van belemmering van de gerechtelijke onderzoeken of procedures en ter vermindering 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 boa moet verplicht een Wpg e-learning volgen. Pas nadat NatuurNetwerk BV het succesvol afronden van de cursus heeft gecontroleerd verleent zij de medewerker toegang tot BRS.

Boa's die al in dienst zijn worden aanvullend getraind voor bewustwording rondom de omgang met politiegegevens. Dit gebeurt in de vorm van een aanvullende training die extern is belegd.

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 Wpg privacy-verklaring die, evenals dit beleid, op de website van de gemeente Papendrecht is te vinden zal zijn.