

Beleidsplan met Beleidsregels Wet politiegegevens 2026 gemeente Nieuwkoop

Burgemeester en wethouders van Nieuwkoop maken bekend dat zij in hun vergadering van 16 december 2025 de Beleidsnota met Beleidsregels Wet politiegegevens gemeente Nieuwkoop 2026 hebben vastgesteld.

Deze nota bevat de uitgangspunten op welke wijze de gemeente Nieuwkoop omgaat met de Wet politiegegevens voor het verwerken van privacygevoelige gegevens, waar het gaat om het vastleggen van, omgaan met en delen van politiegegevens bij de opsporing van strafbare feiten in het kader van haar toezichts- en handhavingstaken door gemeentelijke Boa's.

Het Beleidsplan met de beleidsregels treedt in werking per 1 januari 2026.

1 INLEIDING

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

Voor het houden van toezicht op en handhaven van de openbare orde heeft de gemeente Nieuwkoop Boa's in dienst. Daarbij verwerken de Boa's persoonsgegevens. De verwerking van persoonsgegevens door buitengewoon opsporingsambtenaren (boa's) valt niet alleen onder de AVG maar ook onder de Wet politiegegevens (Wpg).

Boa's verwerken politie-/strafrechtelijke gegevens onder de Wet politiegegevens (hierna: Wpg) in het kader van hun specifieke opsporingsbevoegdheid. Het verwerken van gegevens betreft elke handeling met een politiegegeven; dit zijn o.a. het registreren, raadplegen, wijzigen, tonen, verstrekken en verwijderen van gegevens. De boa's vallen bij de verwerking van die gegevens dus niet onder de AVG, maar onder de Wpg. De Wpg biedt evenwicht tussen de bescherming van de privacy van de burger enerzijds en het belang van de rechtshandhaving anderzijds.

Naast de Wpg zijn ook een aantal andere regelingen van toepassing op de verwerking van politiegegevens, zoals het Besluit politiegegevens (Bpg), Besluit politiegegevens boa (Bpg boa) 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 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.

De gemeente Nieuwkoop is als werkgever verwerkingsverantwoordelijke in het kader van de Wpg. Het is wenselijk de privacyverplichtingen van de Boa's uit de Wpg in beleid vast te leggen. Dit beleid is van toepassing op de boa's die in dienst zijn van de gemeente Nieuwkoop en alle processen, onderdelen, objecten, verwerkingen en gegevensverzamelingen waarin politiegegevens worden verwerkt.

Het Wpg beleid van de gemeente Nieuwkoop is in lijn met het algemene beleid van de gemeente (zoals het strategisch informatiebeveiliging- en privacybeleid) en de relevante lokale, regionale, nationale en Europese wet- en regelgeving.

Daarnaast is dit beleid afgestemd met het werk van de Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten [in licentie onder: CC BY-NC-SA 4.0.].

2 DOELSTELLINGEN VAN HET PRIVACYBELEID

De Wpg kent een aantal verplichtingen. Met dit beleid wil de gemeente Nieuwkoop zich conformeren aan deze verplichtingen. 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, meer in het bijzonder voor documentatie, noodzakelijkheid, rechtmatigheid, doelbinding, juistheid, volledigheid en bewaartermijnen.
- 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 FG ziet er jaarlijks toe op de naleving van de wettelijke regels en het gemeentelijke beleid door alle functionarissen die voor de gemeente politiegegevens verwerken.

2.1 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 iedere 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 CityControl, het digitale systeem, dat door de gemeente Nieuwkoop is aangeschaft bij Sigmax Law Enforcement.

- 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 (onder andere 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 verlenging van het contract voor het gebruik van CityControl. In 2025 is weer een externe audit uitgevoerd.

2.2 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 asterisk (*) 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 worden opgenomen in het verwerkingsregister Fully in Control en voor het aanbrengen mutaties hierin, wordt een werkinstructie opgesteld.

2.3 INFORMATIEBEVEILIGINGSBELEID

De gemeente Nieuwkoop heeft een eigen informatiebeveiligingsbeleid. Dat is vastgelegd in richtinggevend en kaderstellende beleidsdocumenten. De informatiebeveiliging binnen de gemeente Nieuwkoop vindt plaats volgens de algemeen erkende overheidsnorm (BIO). Onderdeel van de informatiebeveiliging bij de gemeente Nieuwkoop zijn onder andere:

- Eigen controles of eigen mededelingen over de beveiligingsmaatregelen
- Jaarlijkse ENSIA-verantwoording
- ICT-Beheerplan 2021-2025
- Gegevensbeschermingsbeleid 2023-2027
- Strategisch Informatiebeveiligingsbeleid 2025-2028
- Jaarlijkse Informatiebeveiligingsplannen

Het gemeentelijke Informatiebeveiligingsbeleid is hiermee actueel en toereikend.

2.4 FG EN BEVOEGD FUNCTIONARIS

2.4.1 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 Nieuwkoop 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.

2.4.2 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.

Persoonsgegevens die verwerkt worden in het kader van de dagelijkse opsporingstaak, vallen onder artikel 8 van de Wpg. Dit gaat over zaken als wildplassen, foutief aanbieden van afval, alcohol gebruiken op de openbare weg en loslopende honden. Ook proces-verbaal opmaken bij onrechtmatig afgeschoten wild of tuinafvaldump valt hieronder. De gegevens kunnen zowel over verdachten, slachtoffers als andere betrokkenen gaan. De werkzaamheden van de BOA's in de gemeente Nieuwkoop richten zich in de praktijk vrijwel uitsluitend op toezicht en handhaving op deze categorie van overtredingen.

Artikel 9 Wpg maakt het mogelijk om gegevens te verwerken die specifiek gericht zijn op bepaalde personen of concrete gebeurtenissen. De inbreuk op de privacy is bij deze verwerkingen groter dan bij artikel 8. Het gaat hier bijvoorbeeld om onderzoeken waarbij bijzondere opsporingsbevoegdheden worden ingezet, zoals het plaatsen van een baken onder een auto bij verdenking van stroperij of stelsmatige observatie bij verdenking van een milieudelict. Opsporingsonderzoek met meer inbreuk op privacy is in de gemeente Nieuwkoop primair het domein van de politie, de Omgevingsdienst West-Holland, en / of andere samenwerkingspartijen met opsporingsbevoegdheden. Daarmee ontbreekt de noodzaak om de gemeentelijke BOA's op basis van artikel 9 Wpg zelfstandig persoonsgegevens te laten verwerken.

De gemeente Nieuwkoop maakt voor de opsporing van strafbare feiten ook geen gebruik van de methode profilering en wil dat ook niet doen. Afgezien daarvan is dat voor de aard van de taken en de BOA-werkzaamheden ook volstrekt niet nodig.

Om daar geen misverstanden over te hebben sluiten wij geautomatiseerd vergelijken en in combinatie zoeken van (persoons-)gegevens en verwerkingen op basis van de artikelen 9 en 13 Wpg expliciet uit.

2.5 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 gelijklopend. Ten behoeve van verzoeken op grond van de Wpg wordt een digitale ingang gerealiseerd via de website van de gemeente Nieuwkoop.

2.6 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 op te nemen in het verwerkingsregister, wordt gebruik gemaakt van CityControl van Sigmax. Bij gebruik van CityControl worden, voor zover mogelijk, de verwerkings- en bewaartermijnen geautomatiseerd toegepast. De gemeente Nieuwkoop maakt voor de opsporing van strafbare feiten geen gebruik van de methode profilering en wil dat ook niet doen. Afgezien daarvan is dat voor de aard van de taken en de BOA-werkzaamheden ook volstrekt niet nodig. Geautomatiseerd vergelijken en in combinatie zoeken van (persoons-)gegevens en verwerkingen op basis van de artikelen 9 en 13 Wpg sluiten wij voor alle duidelijkheid expliciet uit.

Categorie	Termijn verwerking en bewaring	Motivatie
Gegevens Boa	Variabel – Zolang de Boa gebruikt maakt van CC, of indien van toepassing, gedurende de periode van een klacht of verzetszaak.	Om gebruik te kunnen maken van CC 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 politietaak worden verwerkt gedurende 1 jaar. - De verwijderde Politiegegevens worden gedurende 5 jaar bewaard voor afhandeling van klachten, verantwoording van verrichtingen, in bijzondere gevallen en na opdracht van het bevoegd gezag, voor het hernieuwd verwerken waarna zij worden vernietigd.	Artikel 8, lid 1, 2 en 6 jo. artikel 14, lid 1 Wpg
Gegevens mutatie	Onbeperkt	Zolang het incident geregistreerd staat in CC 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 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 Wpg.
Systeem en Error-logging	Variabel – Zolang incident 'actief' is ingevolge artikel 8 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 Wpg.

Gebruikslogging	Variabel – Zolang incident ‘actief’ is ingevolge artikel 8 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 Wpg.
-----------------	---	---

Tabel 1, Termijnen verwerking en bewaring politiegegevens

2.7 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 primair aansluiting gezocht bij de Verstrekkingwijzer van de politie, secundair ook bij de BRS-Verstrekkingwijzer Wpg voor boa's.

2.8 HET MELDEN VAN DATALEKKEN

De datalek-procedure onder de AVG staat 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 Nieuwkoop 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 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. 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.

2.9 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 de training succesvol is afgerond verleent de gemeentelijke functioneel beheerder de medewerker toegang tot CityControl.

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.

2.10 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 Nieuwkoop is te vinden zal zijn.

3 BELEIDSREGELS WPG

Artikel 1 Begripsbepalingen

In dit beleid wordt verstaan onder:

- gemeente Nieuwkoop: het college van de burgemeester en wethouders als verwerkingsverantwoordelijke van de politiegegevens;
- buitengewoon opsporingsambtenaar: de buitengewoon opsporingsambtenaar (boa) als bedoeld in het Besluit buitengewoon opsporingsambtenaar;
- opsporingstaak: de opsporing van de strafbare feiten als bedoeld in artikel 142, tweede lid, van het Wetboek van Strafvordering;

- d. akte van opsporingsbevoegdheid: de akte van opsporingsbevoegdheid als bedoeld in artikel 142, eerste lid, onder a, van het Wetboek van Strafvordering;
- e. wet: de Wet politiegegevens (Wpg), het Besluit politiegegevens, het Besluit politiegegevens voor buitengewoon opsporingsambtenaar en de Regeling periodieke audit politiegegevens;
- f. beschikbaar studiemateriaal: het Praktijkhandboek van de wet politiegegevens, de Verstrekkingenwijzer en het Naslagwerk Verstrekken op grond van de wet politiegegevens;
- g. Wpg-domein: domein bestaande uit de politie, marechaussee, rijksrecherche, Bijzondere Opsporingsdiensten en de buitengewoon opsporingsambtenaren;
- h. politiegegevens: persoonsgegevens die in het kader van de uitoefening van de politietaak worden verwerkt;
- i. verwerken van politiegegevens: elke handeling of elk geheel van handelingen met betrekking tot politiegegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, vergelijken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van politiegegevens;
- j. autorisatiebeleid: het autorisatiebeleid voor het toewijzen, wijzigen en intrekken van autorisaties t.b.v. de toegang tot politiegegevens;
- k. verwerker van politiegegevens: degene die, niet werkzaam binnen de gemeentelijke organisatie, het geheel of een gedeelte van het geautomatiseerde systeem onder zich heeft waarmee de politiegegevens worden verwerkt.
- l. boa-applicatie: het systeem/de applicatie waarin boa's de politiegegevens verwerken.

Artikel 2 Het aanwijzen van de buitengewoon opsporingsambtenaar

- 1. De gemeente Nieuwkoop wijst de buitengewoon opsporingsambtenaar aan, indien de buitengewoon opsporingsambtenaar in het bezit is van een:
 - a. akte van opsporingsbevoegdheid;
 - b. verklaring omtrent het gedrag;
- 2. De buitengewoon opsporingsambtenaar voldoet aan de her- en bijscholingsplicht.
- 3. De gemeente Nieuwkoop organiseert ten aanzien van politiegegevens bewustwordingsactiviteiten dan wel cursussen over de omgang met politiegegevens, die door de buitengewoon opsporingsambtenaar jaarlijks verplicht worden bijgewoond.

Artikel 3 Het verlenen, wijzigen en beëindigen van de toegang tot politiegegevens (artikel 6 van de Wet politiegegevens)

- 1. De gemeente Nieuwkoop stelt ten aanzien van het verlenen, wijzigen- en beëindigen van toegang tot politiegegevens een autorisatiebeleid vast of maakt gebruik van het autorisatiebeleid van de boa-applicatie.
- 2. De gemeente Nieuwkoop verleent aan de buitengewoon opsporingsambtenaar conform het vastgestelde autorisatiebeleid een autorisatie tot politiegegevens, indien de toegang tot politiegegevens noodzakelijk is voor het uitvoeren van de aan de buitengewoon opsporingsambtenaar opgedragen opsporingstaak.
- 3. De gemeente Nieuwkoop wijst de buitengewoon opsporingsambtenaar ten aanzien van politiegegevens op de plicht tot geheimhouding en de consequenties bij de schending van deze plicht.
- 4. Indien de buitengewoon opsporingsambtenaar van functie verandert dan wel uit dienst gaat, wordt de autorisatie conform het autorisatiebeleid gewijzigd of beëindigd.

Artikel 4 De plicht tot loggen (artikel 32a van de Wet politiegegevens)

- 1. De gemeente Nieuwkoop controleert en evalueert periodiek de toegekende autorisaties van de buitengewoon opsporingsambtenaar met als doel om de integriteit en de rechtmatigheid van de toegang tot politiegegevens te waarborgen.
- 2. De verwerker heeft ten aanzien van de periodieke controle de plicht om de toegang tot politiegegevens te loggen.
- 3. De verwerker verstrekt op verzoek van de gemeente Nieuwkoop de logginggegevens zodat deze conform het autorisatiebeleid periodiek gecontroleerd kunnen worden.
- 4. De gemeente Nieuwkoop gebruikt de logginggegevens uitsluitend voor de controle van de rechtmatigheid van de gegevensverwerking, ter ondersteuning van de verplichte audits en ter waarborging van de integriteit en de rechtmatigheid van de toegang tot politiegegevens.
- 5. De gemeente Nieuwkoop legt het resultaat van de periodieke controle vast in een verslag van bevindingen, welke wordt gearchiveerd binnen het daartoe bestemde en beveiligde zaakstelsel.
- 6. De gemeente Nieuwkoop bewaart de logginggegevens en het resultaat van de periodieke controle hierop voor een periode van vijf jaar.

Artikel 5 Het verwerken van politiegegevens

1. De gemeente Nieuwkoop voorziet in werkinstructies per boa-domein, die de buitengewoon opsporingsambtenaar bij de uitvoering van de opsporingstaak in acht neemt.
2. De buitengewoon opsporingsambtenaar verwerkt politiegegevens ten behoeve van de uitvoering van de politietaak als bedoeld in artikel 8 van de Wet politiegegevens.
3. De buitengewoon opsporingsambtenaar verwerkt geen politiegegevens, indien het gegevens betreft die niet noodzakelijk zijn voor de uitvoering van de aan hem of haar opgedragen opsporingstaak.
4. De buitengewoon opsporingsambtenaar verwerkt geen politiegegevens buitenom de boa-applicatie in zogenoemde schaduwsystemen.
5. De buitengewoon opsporingsambtenaar maakt bij het verwerken van politiegegevens onderscheid tussen:
 - a. de verschillende categorieën van betrokkenen zoals genoemd in artikel 6b van de Wet politiegegevens;
 - b. gegevens die gebaseerd zijn op feiten en een persoonlijk oordeel zoals genoemd in artikel 4 van de Wet politiegegevens.
6. De verwerker dient ervoor te zorgen dat het onderscheid zoals genoemd in het vijfde lid en onder a van dit artikel in de boa-applicatie, waartoe de buitengewoon opsporingsambtenaar toegang heeft, mogelijk wordt gemaakt.
7. De buitengewoon opsporingsambtenaar neemt geen besluiten die uitsluitend gebaseerd zijn op geautomatiseerde verwerking zoals bedoeld in artikel 7a van de Wet politiegegevens, met inbegrip van profilering, dat voor de betrokkene nadelige rechtsgevolgen heeft of hem of haar in aanmerkelijke mate treft.

Artikel 6 De termijnen van politiegegevens (artikel 14 van de Wet politiegegevens)

1. De gemeente Nieuwkoop voorziet in voldoende waarborgen om te bewerkstelligen dat de politiegegevens conform de wet niet langer worden bewaard dan strikt noodzakelijk is voor de uitvoering van de buitengewoon opsporingsambtenaar opgedragen opsporingstaak.
2. De gemeente Nieuwkoop zorgt ervoor dat de politiegegevens voor de uitvoering van de opsporingstaak zoals bedoeld in artikel 8 van de Wet politiegegevens:
 - a. gedurende een jaar beschikbaar zijn in het kader van de uitvoering van de opsporingstaak;
 - b. na een jaar slechts beschikbaar zijn voor het gericht zoeken;
 - c. na vijf jaar worden verwijderd;
 - d. na tien jaar worden vernietigd.
3. De verwerker zorgt ervoor dat de bewaartermijn conform de wet en het tweede lid van dit artikel geconfigureerd zijn, zodat gewaarborgd is dat de politiegegevens niet langer worden bewaard dan strikt noodzakelijk is voor de uitvoering van de opsporingstaak.
4. De buitengewoon opsporingsambtenaar neemt de termijnen conform de wet en het tweede lid van dit artikel in acht.

Artikel 7 Het ter beschikking stellen en verstrekken van politiegegevens (artikel 15 en paragraaf 3 van de Wet politiegegevens)

1. De gemeente Nieuwkoop stelt de 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.
2. De gemeente Nieuwkoop mag de politiegegevens verstrekken zoals beschreven in de verstrekkingswijzer aan partijen buiten het Wpg-domein. Daarbij wijst de gemeente Nieuwkoop de ontvangende partij op de plicht tot geheimhouding die op de verstrekte gegevens van toepassing is.
3. De gemeente Nieuwkoop legt de verstrekking zoals genoemd in het tweede lid van dit artikel vast. (artikel 32, eerste lid aanhef en onder b, van de Wet politiegegevens)
4. De verwerker heeft ten aanzien van het tweede lid van dit artikel de plicht om binnen de gebruikte applicaties, technische mogelijkheden te creëren, waarmee verstrekkingen kunnen worden vastgelegd. (artikel 32, eerste lid aanhef en onder b van de Wet politiegegevens)
5. De verwerker dient ervoor te zorgen dat de geautomatiseerde verstrekkingen, zoals bijvoorbeeld aan het Centraal Justitieel Incassobureau (CJIB), conform de wet plaatsvinden en worden gedocumenteerd.
6. De gemeente Nieuwkoop alsmede de verwerker voorzien in de technische mogelijkheden om ervoor te zorgen dat de politiegegevens door middel van een beveiligde wijze worden verstrekt aan de ontvangende partij.
7. De gemeente Nieuwkoop verstrekt geen politiegegevens aan ontvangers in derde landen of internationale organisaties.

Artikel 8 De rechten van de betrokkenen (paragraaf 4 van Wet politiegegevens)

1. De gemeente Nieuwkoop draagt zorg voor het informeren van de betrokkenen over de verwerking van politiegegevens. Dit vindt plaats conform paragraaf 4 van de Wet politiegegevens. Daarbij heeft de gemeente Nieuwkoop de plicht tot:
 - a. actieve informatieverstrekking waarbij de informatievoorziening op de website conform de wet plaatsvindt;
 - b. passieve informatieverstrekking; waarbij de informatie op verzoek wordt verstrekt, tenzij het verzoek conform artikel 27 van de Wet politiegegevens geheel of gedeeltelijk kan worden afgewezen, bijvoorbeeld als de informatieverstrekking de opsporing en vervolging belemmert.
2. De gemeente Nieuwkoop stelt conform de wet een procedure vast voor de behandeling van verzoeken van betrokkenen, bestaande uit:
 - a. recht op informatie; betrokkenen moeten erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden verwerkt. Betrokkenen worden door de gemeente geïnformeerd op het moment dat zijn/ haar persoonsgegevens worden verwerkt.
 - b. recht op inzage; betrokkenen hebben de mogelijkheid om in te zien of, en op welke manier, zijn/ haar politiegegevens worden verwerkt.
 - c. recht op rectificatie; als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene op een verzoek indienen bij de gemeente om dit te corrigeren.
 - d. recht op vernietiging; betrokkenen hebben het recht om politiegegevens te laten verwijderen. De gemeente stelt eventuele partners van de gemeente als deze de gegevens ook hebben, op de hoogte dat de betrokkene een verwijderingsverzoek heeft ingediend.
 - e. recht op bezwaar.

Artikel 9 Het behandelen van datalekken (artikel 33a van de Wet politiegegevens)

1. De gemeente Nieuwkoop stelt conform de wet een procedure vast voor het melden van een (vermoedelijke) inbreuk op de beveiliging op politiegegevens, waaronder voor het melden van datalekken.
2. De gemeente Nieuwkoop houdt een register bij van gemelde datalekken.

Artikel 10 Het register van verwerkingen (artikel 31d van de Wet politiegegevens)

1. De gemeente Nieuwkoop houdt een register van verwerkingen bij, waarin per verwerking minimaal de volgende informatie voorkomt:
 - a. de naam en contactgegevens van de gemeente Nieuwkoop;
 - b. de verwerkingsdoeleinden;
 - c. een beschrijving van de categorieën persoonsgegevens die worden verwerkt;
 - d. een beschrijving van de categorieën betrokkenen;
 - e. een beschrijving van de categorieën van ontvangers aan wie de politiegegevens ter beschikking worden gesteld of worden verstrekt;
2. De gemeente Nieuwkoop actualiseert jaarlijks het register van verwerkingen.

Artikel 11 Het uitvoeren van een audit (artikel 33 van de Wet politiegegevens)

1. De gemeente Nieuwkoop laat conform de wet, eenmaal in de vier jaren een externe audit uitvoeren.
2. De gemeente Nieuwkoop voert ter voorbereiding op de verplichting in het eerste lid van dit artikel, jaarlijks een interne audit uit, of laat deze uitvoeren door een externe auditor.
3. De gemeente Nieuwkoop stelt ten behoeve van het tweede lid van dit artikel een auditplan vast.
4. De betrokken verwerkers dienen ten behoeve van de audit een Third Party Memorandum verklaring te overleggen die conform de 'Nederlandse Orde van EDP Auditors handreiking' wordt uitgevoerd, zodat deze verklaring betrokken kan worden bij de beoordeling van de audit.
5. Indien uit de resultaten van de audit, zoals bedoeld in het eerste lid van dit artikel, blijkt dat de verwerking van de politiegegevens op onderdelen niet voldoet aan de wettelijke normen, dient de gemeente Nieuwkoop binnen een jaar zorg te dragen voor deze tekortkomingen, met als doel dat deze worden verholpen. Daarnaast voert de gemeente Nieuwkoop binnen één jaar een hercontrole uit, binnen de onderdelen waarvan het resultaat onvoldoende bleek te zijn.
6. Indien blijkt dat de beheersmaatregelen ten aanzien van de gebruikte applicatie(s) niet voldoen aan de wettelijke normen, dan draagt de verwerker verantwoordelijkheid voor het verhelpen van de tekortkomingen binnen een periode van één jaar.
7. De gemeente Nieuwkoop zendt een afschrift van de controleresultaten van de audit zoals bedoeld in het eerste lid van dit artikel aan de Autoriteit Persoonsgegevens.

Artikel 12 De functionaris gegevensbescherming (artikel 36 van de Wet politiegegevens)

1. De gemeente Nieuwkoop stelt een functionaris gegevensbescherming aan ten behoeve van de controle en het toezicht op het verwerken van politiegegevens conform de wet en het beleid van de gemeente Nieuwkoop.
2. De functionaris gegevensbescherming voert daarbij periodiek controles uit op het naleven van de wettelijke verplichtingen, waaronder de controle op:
 - a. de bewustwordingsverplichting conform het derde lid van artikel 1 van dit beleid;
 - b. het autorisatieproces conform artikel 2 van dit beleid;
 - c. de kwaliteit en waarborging van de juistheid van de nauwkeurigheid van politiegegevens;
 - d. het verwerken van politiegegevens conform artikel 5 van dit beleid;
 - e. de bewaartermijnen conform artikel 6 van dit beleid;
 - f. het ter beschikking stellen en verstrekken van politiegegevens zoals bedoeld in artikel 7 van dit beleid;
 - g. de controle op de informatiebeveiliging en de controle op het uitvoeren van een risicoanalyse zoals genoemd artikel 8 van dit beleid;
 - h. het register voor verwerkingen conform artikel 11 van dit beleid;
 - i. de verplichtingen ten aanzien van de audit conform artikel 12 van dit beleid.
3. De functionaris gegevensbescherming stelt jaarlijks een verslag op.

Artikel 13 De verplichtingen van de gemeente Nieuwkoop

1. De gemeente Nieuwkoop draagt zorg dat de procesinrichting voor de verwerking van politiegegevens in opzet, bestaan en dat de werking voldoet zoals genoemd in de wet, zodat hierop door de auditor en de functionaris gegevensbescherming toezicht kan worden gehouden.
2. De gemeente Nieuwkoop treft daarbij conform de wet passende technische- en organisatorische maatregelen om ongeoorloofde of onrechtmatige verwerkingen, verlies, vernietiging of beschadiging van politiegegevens tegen te gaan, met als doel om de rechtmatigheid en beveiliging van politiegegevens te waarborgen (artikel 4a en 4b van de Wet politiegegevens).
3. Indien er sprake is van een hoog risico op de rechten en vrijheden van betrokkenen, dan voert de gemeente Nieuwkoop conform artikel 4c van de Wet politiegegevens een risicoanalyse, zoals een Data protection impact assessment (DPIA), uit.
4. De gemeente Nieuwkoop maakt uitsluitend gebruik van een verwerker, indien de verwerker afdoende garandeert dat de passende technische- en organisatorische maatregelen en procedures zodanig worden geïmplementeerd dat voldaan wordt aan het bij of krachtens de wet bepaalde (Artikel 6c, 4a en 4b van de Wet politiegegevens).
5. De verwerker verstrekt op verzoek van de gemeente Nieuwkoop alle informatie die nodig is om de nakoming van de verplichtingen uit artikel 6, 32 en 32a van de Wet politiegegevens aan te tonen.
6. De gemeente Nieuwkoop legt de verplichtingen zoals genoemd in het vijfde lid van dit artikel, vast in een schriftelijke overeenkomst, welke door beide partijen wordt ondertekend. (artikel 6c, tweede lid, van de Wet politiegegevens)
7. De gemeente Nieuwkoop voldoet aan de documentatieplicht zoals genoemd in de wet. (artikel 32, eerste lid, van de wet Politiegegevens)

Artikel 15 Uitsluitingen

De gemeente Nieuwkoop maakt geen gebruik van:

- a. geautomatiseerd vergelijken en in combinatie zoeken (artikel 11 van de Wet politiegegevens).
- b. artikel 9-verwerkingen (artikel 9 van de Wet politiegegevens).
- c. artikel 13-verwerkingen (artikel 13 van de Wet politiegegevens).

Artikel 16 Strategisch informatiebeveiligings- en privacybeleid

1. Het strategisch informatiebeveiligings- en privacybeleid is vastgesteld in een richtinggevend en kaderstellend beleidsdocument, welke eens per 4 jaar wordt vastgesteld door het college. De gemeente Nieuwkoop vult het aan met beleid voor informatiebeveiliging op tactisch en operationeel niveau met specifieke (beleids) documenten
2. Het informatiebeveiligingsbeleid geldt voor alle activiteiten van de gemeente. 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 risico analyse waaruit het risico niveau blijkt met betrekking tot ongeoorloofde en onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging. Deze maatregelen moeten bovendien periodiek worden geëvalueerd en zo nodig geactualiseerd.

Artikel 17 Evaluatie beleid

Dit Wpg-beleid wordt minimaal één keer per vier jaar getoetst, of eerder indien nodig vanwege strategische ontwikkelingen, ontwikkelingen in de samenleving of verplichtingen voortvloeiend uit wet- en regelgeving.

Artikel 18. Citeertitel en inwerkingtreding

1. Deze beleidsregels treden inwerking met ingang van 1 januari 2026. Het besluit wordt gepubliceerd in het Gemeenteblad.
2. Deze beleidsregels worden aangehaald als "Beleid Wet politiegegevens gemeente Nieuwkoop".

Aldus vastgesteld op 16 december 2025

Burgemeester en wethouders van Nieuwkoop,

*de secretaris,
Nicolette Caspers*

*de burgemeester
Robbert-Jan van Duijn*

4 TOELICHTING – ARTIKELGEWIJS

4.1 'FREE FLOW OF INFORMATION' PRINCIPE (ARTIKEL 7)

Vrij delen van informatie is uitgangspunt van de Wet politiegegevens. Dat principe strekt ertoe dat informatie in principe gedeeld moet worden tussen organisaties die die informatie nodig hebben voor hun wettelijke taken. Voor het delen moet wel een wettelijke basis zijn en er gelden strikte voorwaarden voor, zoals noodzakelijkheid, proportionaliteit en er mag geen minder ingrijpende manier zijn om het doel te bereiken (subsidiariteitsbeginsel).

4.2 UITSLUITINGEN (ARTIKEL 15)

Persoonsgegevens die verwerkt worden in het kader van de dagelijkse opsporingstaak, vallen onder artikel 8 van de Wpg. Dit gaat over zaken als wildplassen, foutief aanbieden van afval, alcohol gebruiken op de openbare weg en loslopende honden. Ook proces-verbaal opmaken bij onrechtmatig afgeschoten wild of tuinafvaldump valt hieronder. De gegevens kunnen zowel over verdachten, slachtoffers als andere betrokkenen gaan. De werkzaamheden van de BOA's in de gemeente Nieuwkoop richten zich in de praktijk vrijwel uitsluitend op toezicht en handhaving op deze categorie van overtredingen.

Artikel 9 Wpg maakt het mogelijk om gegevens te verwerken die specifiek gericht zijn op bepaalde personen of concrete gebeurtenissen. De inbreuk op de privacy is bij deze verwerkingen groter dan bij artikel 8. Het gaat hier bijvoorbeeld om onderzoeken waarbij bijzondere opsporingsbevoegdheden worden ingezet, zoals het plaatsen van een baken onder een auto bij verdenking van stroperij of stelselmatige observatie bij verdenking van een milieudelict. Opsporingsonderzoek met meer inbreuk op privacy is in de gemeente Nieuwkoop primair het domein van de politie, de Omgevingsdienst West-Holland, en / of andere samenwerkingspartijen met opsporingsbevoegdheden. Daarmee ontbreekt de noodzaak om de gemeentelijke BOA's op basis van artikel 9 Wpg zelfstandig persoonsgegevens te laten verwerken.

De gemeente Nieuwkoop maakt voor de opsporing van strafbare feiten ook geen gebruik van de methode profilering en wil dat ook niet doen. Afgezien daarvan is dat voor de aard van de taken en de BOA-werkzaamheden ook volstrekt niet nodig.

Om daar geen misverstanden over te hebben zijn toepassingen van geautomatiseerd vergelijken en in combinatie zoeken van (persoons-)gegevens en verwerkingen op basis van de artikelen 9 en 13 Wpg expliciet uitgesloten.