Waterschap Noorderzijlvest

WATERSCHAPSBLAD

Officiële uitgave van het dagelijks bestuur van het Waterschap Noorderzijlvest

Nr. 28603

2 november 2026

BELEID WET POLITIEGEGEVENS (WPG)

INHOUDSOPGAVE

1 Inleiding
2 Wettelijk kader
3 Grondslagen voor verwerking
4 Categorieën van politiegegevens
5 Organisatie en verantwoordelijkheden
6 Autorisatiebeleid
7 Technische en organisatorische maatregelen
8 Register van verwerkingen
9 Documentatie en dossiervorming
10 Verstrekking en ter beschikking stelling
11 Bewaartermijnen en vernietiging
12 Rechten van betrokkenen
13 Data Protection Impact Assessment (DPIA)
14 Datalekken
15 Verwerkers en derden
16 Bewustwording en training
17 Interne en externe audits
18 Toezicht en verantwoording
19 Incidentenbeheer en escalatie
20 Evaluatie en actualisatie van beleid
21 Slotbepalingen
22 Gelieerde documenten

1 INLEIDING

1.1 Aanleiding en doel

De Wet politiegegevens (Wpg) regelt de verwerking van persoonsgegevens in het kader van opsporings- en handhavingstaken door buitengewoon opsporingsambtenaren (boa's). Waterschap Noorderzijlvest heeft boa's in dienst die belast zijn met het opsporen van overtredingen van onder andere de Waterschapsverordening, milieuregels en andere relevante wet- en regelgeving.
Dit beleid heeft tot doel te waarborgen dat het waterschap de verwerking van politiegegevens op rechtmatige, behoorlijke en transparante wijze uitvoert, conform de wettelijke verplichtingen uit de Wpg. Het beleid vormt het kader voor alle verwerkingsactiviteiten waarbij politiegegevens betrokken zijn en draagt bij aan de bescherming van de privacy en de rechten van betrokkenen.

1.2 Reikwijdte

Dit beleid is van toepassing op:

- Alle boa's in dienst van het waterschap
- Alle medewerkers die betrokken zijn bij de verwerking van politiegegevens
- Alle afdelingen, processen en systemen waarbij politiegegevens worden verwerkt
- Alle verwerkingsactiviteiten in het kader van de uitvoering van de dagelijkse politietaak en specifieke onderzoeken (zoals bedoeld in hoofdstuk 9.3 van dit beleid)

1.3 Relatie tot andere beleidsstukken

Dit beleid vormt een aanvulling op het algemene privacy- en informatiebeveiligingsbeleid van het waterschap en moet worden gelezen in samenhang met:

- Algemene Verordening Gegevensbescherming (AVG)
- Baseline Informatiebeveiliging Overheid (BIO, zie 7.1)
- Informatieveiligheid en privacybeleid van waterschap Noorderzijlvest
- Privacybeleid waterschap Noorderzijlvest
- Procedure datalekken waterschap Noorderzijlvest

1.4 Begripsbepalingen

Voor de toepassing van dit beleid wordt verstaan onder:
Politiegegeven: Een persoonsgegeven of bijzonder persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de opsporingstaak door boa's van het waterschap.
Verwerking: Elke handeling of elk geheel van handelingen met betrekking tot politiegegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken, verspreiden, ter beschikking stellen, aligneren, combineren, afschermen, verwijderen of vernietigen van gegevens.
Verwerkingsverantwoordelijke: Waterschap Noorderzijlvest, vertegenwoordigd door het dagelijks bestuur.
Functionaris Gegevensbescherming (FG): De functionaris, belast met toezicht op de naleving van de Wpg binnen het waterschap.
Betrokkene: De natuurlijke persoon op wie een politiegegeven betrekking heeft.
Boa: Buitengewoon opsporingsambtenaar in dienst van het waterschap, bevoegd tot opsporing van strafbare feiten op grond van artikel 142 Wetboek van Strafvordering.
Dagelijkse politietaak: De verwerking van politiegegevens die noodzakelijk is voor de uitvoering van reguliere opsporings- en handhavingstaken.
Specifiek onderzoek: De verwerking van politiegegevens in het kader van een afgebakend onderzoek met een bepaald doel en beperkte looptijd.

2 WETTELIJK KADER

2.1 Wet politiegegevens

De Wpg is van toepassing op de verwerking van politiegegevens door boa's van het waterschap. De wet stelt eisen aan de rechtmatigheid, doelbinding, dataminimalisatie, juistheid, bewaartermijnen en beveiliging van politiegegevens.

2.2 Relatie met AVG en BIO

De Wpg kent raakvlakken met de AVG, zoals de meldplicht datalekken, het uitvoeren van Data Protection Impact Assessments (DPIA's) en het aanstellen van een Functionaris Gegevensbescherming. Voor aspecten die niet expliciet in de Wpg zijn geregeld, zijn de bepalingen uit de AVG van overeenkomstige toepassing.
Voor de technische en organisatorische beveiliging van politiegegevens hanteert het waterschap de Baseline Informatiebeveiliging Overheid (BIO) als uitgangspunt.

2.3 Auditverplichtingen

Op grond van artikel 33 Wpg is het waterschap verplicht om minimaal eens per vier jaren een externe privacy audit te laten uitvoeren door een onafhankelijke auditor conform het controleprotocol van NOREA (De beroepsorganisatie van IT-auditors). Daarnaast dienen jaarlijks interne audits te worden uitgevoerd.

3 GRONDSLAGEN VOOR VERWERKING

3.1 Rechtmatige grondslagen

Het waterschap mag politiegegevens uitsluitend verwerken indien sprake is van een wettelijke grondslag zoals bedoeld in artikel 10 Wpg. Voor het waterschap zijn de volgende grondslagen van toepassing:

1. **Uitvoering van de dagelijkse politietaak:** De verwerking is noodzakelijk voor de uitvoering van reguliere opsporings- en handhavingstaken, zoals het opsporen van overtredingen van de Waterschapsverordening en milieuregels.
2. **Specifiek onderzoek:** De verwerking is noodzakelijk voor een specifiek onderzoek met een afgebakend doel en beperkte looptijd.

3.2 Noodzakelijkheidstoets

Voorafgaand aan elke verwerking van politiegegevens toetst de betrokken boa of de verwerking noodzakelijk is voor de uitvoering van zijn taak. Daarbij gelden de volgende principes:

- **Subsidiariteit:** Kan het doel ook worden bereikt zonder verwerking van (bijzondere) persoonsgegevens of met minder ingrijpende middelen?
- **Proportionaliteit:** Staat de verwerking in redelijke verhouding tot het beoogde doel?
- **Doelbinding:** Worden de gegevens uitsluitend verwerkt voor het specifieke doel waarvoor ze zijn verzameld?

De afweging wordt gedocumenteerd in het BOA Registratiesysteem (BRS).

De maatregelen om bovenstaande principes te borgen, zijn onder andere benoemd in Hoofdstuk 7 (Technische en Organisatorische maatregelen), Hoofdstuk 16 (Bewustwording en Training), 17 (Interne en externe audits) en 18 (Toezicht en verantwoording).

Ten tijde van het opstellen van dit beleid is het geautomatiseerd vergelijken en gecombineerd zoeken en verwerken niet noodzakelijk geweest en derhalve niet uitgevoerd. Ditzelfde geldt voor artikel 13 verwerkingen. Mocht het waterschap in de toekomst, in een uitzonderlijk geval, één van bovenstaande toch noodzakelijk achten, dan wordt de Functionaris Gegevensbescherming hiervan op de hoogte gesteld en worden de noodzakelijke maatregelen, zoals het herijken van de DPIA, getroffen.

4 CATEGORIEËN VAN POLITIEGEGEVENS

4.1 Onderscheid feitelijke en persoonlijke gegevens

Bij de verwerking van politiegegevens wordt onderscheid gemaakt tussen:

- Feitelijke gegevens: Gegevens die objectief zijn vast te stellen (bijvoorbeeld: naam, adres, tijdstip overtreding, locatie)
- Persoonlijke gegevens: Gegevens gebaseerd op persoonlijke indrukken of beoordelingen (bijvoorbeeld: gedragsobservaties, inschatting van risico's)

Deze scheiding wordt technisch geborgd in BRS voor de verwerking van politiegegevens.

4.2 Categorieën betrokkenen

Het waterschap onderscheidt bij de verwerking van politiegegevens de volgende categorieën betrokkenen:

- Verdachten
- Burgers
- Getuigen
- Medewerkers

Deze categorisering wordt vastgelegd in het register van verwerkingen en in de systemen waar politiegegevens worden verwerkt.

4.3 Bijzondere categorieën politiegegevens

Bijzondere persoonsgegevens zoals bedoeld in artikel 5 Wpg (onder meer gegevens over ras, etnische afkomst, politieke opvattingen, religie, gezondheid, seksueel gedrag of strafrechtelijke veroordelingen) worden uitsluitend verwerkt indien dit strikt noodzakelijk is voor de uitvoering van de opsporingstaak en indien passende beveiligingsmaatregelen zijn getroffen.
Ten tijde van het opstellen van dit beleid verwerkt het waterschap de hierboven genoemde bijzondere persoonsgegevens niet. Mocht het waterschap in de toekomst, in een uitzonderlijk geval, toch overgaan tot het verwerken van dergelijke persoonsgegevens, dan wordt de Functionaris Gegevensbescherming hiervan op de hoogte gesteld.

5 ORGANISATIE EN VERANTWOORDELIJKHEDEN

5.1 Verwerkingsverantwoordelijke

Waterschap Noorderzijlvest, vertegenwoordigd door het dagelijks bestuur, treedt op als verwerkingsverantwoordelijke in de zin van de Wpg. Het dagelijks bestuur draagt de eindverantwoordelijkheid voor de naleving van de Wpg binnen de organisatie.

5.2 Functionaris Gegevensbescherming

Het waterschap heeft een Functionaris Gegevensbescherming (FG) aangesteld conform artikel 36 Wpg.
De FG is verantwoordelijk voor:

- Toezicht op de naleving van de Wpg binnen de organisatie
- Advisering over DPIA's en andere privacy-vraagstukken
- Fungeren als aanspreekpunt voor betrokkenen en toezichthouders
- Samenwerking met de Autoriteit Persoonsgegevens

5.3 Primair verantwoordelijke managers

De verwerking van politiegegevens vindt plaats binnen afdelingen en processen. Het management van deze afdelingen draagt de primaire verantwoordelijkheid voor een goede verwerking en beveiliging van politiegegevens op hun afdeling.
Verantwoordelijke afdelingen/teams:

- Team Vergunningen en Handhaving

Minimaal vereist is dat het teammanagement op de hoogte is van dit beleid en toeziet op de naleving ervan binnen hun verantwoordelijkheidsgebied.

5.4 Boa's

Elke boa is persoonlijk verantwoordelijk voor:

- Het naleven van dit beleid en de daaruit voortvloeiende procedures
- Het uitsluitend verwerken van politiegegevens voor de uitvoering van zijn wettelijke taak
- Het toepassen van de noodzakelijkheidstoets voorafgaand aan elke verwerking
- Het juist documenteren en registreren van verwerkte politiegegevens
- Het direct melden van (vermoedens van) datalekken conform de procedure datalekken

5.5 Overige medewerkers

Alle medewerkers die op enige wijze betrokken zijn bij de verwerking van politiegegevens (bijvoorbeeld administratieve ondersteuning, ICT-beheerders) zijn verplicht om:

- Dit beleid na te leven
- Vertrouwelijk om te gaan met politiegegevens
- Uitsluitend toegang te nemen tot politiegegevens voor zover dat noodzakelijk is voor hun werkzaamheden
- Geheimhouding in acht te nemen, ook na beëindiging van het dienstverband

6 AUTORISATIEBELEID

6.1 Uitgangspunten

Het waterschap hanteert een autorisatiebeleid op basis van de volgende principes:

- Need to know: Toegang tot politiegegevens wordt uitsluitend verleend aan personen die deze toegang noodzakelijkerwijs nodig hebben voor de uitvoering van hun taken
- Least privilege: Medewerkers krijgen de minimaal benodigde toegangsrechten
- Functiescheiding: Waar mogelijk worden autorisaties gescheiden op basis van functierollen
- Periodiciteit: Autorisaties worden periodiek getoetst en indien nodig herzien

6.2 Autorisatiematrix

Het waterschap houdt een autorisatiematrix bij waarin voor elke functierol is vastgelegd:

- Welke systemen toegankelijk zijn
- Welke gegevens geraadpleegd mogen worden
- Welke handelingen uitgevoerd mogen worden (lezen, schrijven, wijzigen, verwijderen)
- De geldigheid van de autorisatie

6.3 Procedure voor toekenning en intrekking

Autorisaties worden toegekend op basis van een schriftelijk verzoek van de leidinggevende. De procedure is als volgt:

1. De leidinggevende dient een autorisatieverzoek in bij de BRS-beheerder
2. Het verzoek wordt getoetst aan het autorisatiebeleid en de autorisatiematrix
3. Bij goedkeuring wordt de autorisatie technisch doorgevoerd
4. De medewerker ontvangt een bevestiging met de verleende rechten
5. De autorisatie wordt vastgelegd in het autorisatieregister

Autorisaties worden ingetrokken bij:

- Beëindiging van het dienstverband
- Wijziging van functie waarbij toegang niet langer noodzakelijk is
- Misbruik of overtreding van het autorisatiebeleid
- Periodieke herbeoordeling waarbij de noodzaak niet langer aanwezig is

6.4 Periodieke toetsing

Minimaal jaarlijks wordt de autorisatiematrix en het autorisatieregister getoetst door de teamleider Vergunningen en Handhaving. Overtollige of niet langer benodigde autorisaties worden ingetrokken.

7 TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

7.1 Baseline Informatiebeveiliging Overheid (BIO)
Het waterschap hanteert de BIO als uitgangspunt voor de beveiliging van politiegegevens. De BIO-maatregelen worden specifiek toegepast op alle systemen en processen waarbij politiegegevens worden verwerkt.

7.2 Toegangsbeveiliging
De volgende technische toegangsbeveiligingsmaatregelen zijn van toepassing:
- **Authenticatie**: Toegang tot systemen met politiegegevens vereist minimaal tweefactorauthenticatie
- **Encryptie**: Politiegegevens worden tijdens transport en opslag versleuteld
- **Netwerksegmentatie**: Systemen met politiegegevens zijn gescheiden van andere netwerken
- **Fysieke beveiliging**: Werkplekken en opslaglocaties met politiegegevens zijn fysiek beveiligd tegen onbevoegde toegang

7.3 Logging en monitoring
Van alle verwerkingen van politiegegevens wordt automatisch een logregistratie bijgehouden die minimaal de volgende gegevens bevat:
- Gebruikersnaam van degene die de verwerking heeft uitgevoerd
- Datum en tijdstip van de verwerking
- Type verwerking (raadplegen, wijzigen, verstrekken, verwijderen)
- Identificatie van het geraadpleegde gegeven of dossier

Logs worden minimaal 5 jaren bewaard en regelmatig geanalyseerd op ongebruikelijke patronen of onbevoegde toegang.
Verantwoordelijke voor loganalyse: Teammanager Vergunning en Handhaving

7.4 Scheiding van gegevens
Technisch wordt een scheiding aangebracht tussen:
- Gegevens die onder de AVG vallen en gegevens die onder de Wpg vallen
- Feitelijke gegevens en persoonlijke beoordelingen
- Gegevens van verschillende categorieën betrokkenen (verdachten, slachtoffers, getuigen)

Deze scheiding voorkomt onbedoelde vermenging en draagt bij aan doelbinding.

7.5 Back-up en continuïteit
Van politiegegevens worden regelmatige back-ups gemaakt. Back-ups worden op dezelfde wijze beveiligd als de productiegegevens. Maandelijks worden restore testen uitgevoerd om de back-ups en herstelprotocollen te valideren.

8 REGISTER VAN VERWERKINGEN

8.1 Wettelijke verplichting
Op grond van artikel 31d Wpg houdt het waterschap een register bij van alle verwerkingen van politiegegevens. Het register is het centrale overzicht van alle verwerkingsactiviteiten en bevat alle wettelijke vereisten.

8.2 Beheer en actualisatie
Het register wordt beheerd door de Privacy Officer. Het register wordt actueel gehouden door:
- Nieuwe verwerkingen direct toe te voegen
- Gewijzigde verwerkingen bij te werken
- Beëindigde verwerkingen te archiveren
- Periodiek, op basis van het toetsings en auditplan AVG, een integrale controle uit te voeren

8.3 Toegankelijkheid
Het register is toegankelijk voor:
- De Privacy Officer
- De Functionaris Gegevensbescherming (FG)
- Het management van betrokken afdelingen
- Interne en externe auditors
- Toezichthouder (Autoriteit Persoonsgegevens)

9 DOCUMENTATIE EN DOSSIERVORMING

9.1 Documentatieplicht

Van elke verwerking van politiegegevens wordt documentatie bijgehouden die inzicht geeft in:

- Het doel van de verwerking
- De grondslag voor de verwerking
- De verwerkte gegevens en de bron daarvan
- De betrokken personen (categorie betrokkene)
- Eventuele verstrekkingen aan derden
- De bewaartermijn

9.2 Dossiervorming dagelijkse politietaak

Voor de dagelijkse politietaak (zoals bedoeld in artikel 8 van de Wpg) worden dossiers gevormd per zaak of incident. Elk dossier bevat minimaal:

- Een uniek dossiernummer
- Datum en tijdstip van de geconstateerde overtreding
- Beschrijving van de feiten
- Identificatiegegevens van betrokkene(n)
- Genomen maatregelen (waarschuwing, proces-verbaal, bestuurlijke sanctie)
- Eventuele bijlagen (foto's, verklaringen, correspondentie)

Dossiers worden opgeslagen in het BOA Registratie Systeem (BRS).

9.3 Dossiervorming specifiek onderzoek

Ten tijde van het opstellen van dit beleid worden door het waterschap nog geen specifieke onderzoeken, zoals bedoeld in artikel 9 van de Wpg, uitgevoerd. Indien het waterschap dit in een bijzonder geval noodzakelijk acht, wordt de onderstaande procedure gevolgd.
Voor specifieke onderzoeken wordt vooraf een onderzoeksplan opgesteld dat bevat:

- De aanleiding en het doel van het onderzoek
- De verwachte duur van het onderzoek
- De te verwerken categorieën politiegegevens
- De betrokken personen en middelen
- De bewaartermijn na afronding van het onderzoek

Het onderzoeksplan wordt goedgekeurd door de verantwoordelijk manager en de Privacy Officer. Na afronding wordt een eindrapportage opgesteld.

9.4 Kwaliteit en volledigheid

Het waterschap draagt zorg voor de juistheid en volledigheid van de verwerkte politiegegevens. Dit wordt op meerdere manier geborgd, onder andere door de maatregelen benoemd in Hoofdstuk 7 (Technische en Organisatorische maatregelen), Hoofdstuk 16 (Bewustwording en Training), 17 (Interne en externe audits) en 18 (Toezicht en verantwoording).
Onjuiste of onvolledige gegevens worden zo spoedig mogelijk gecorrigeerd. Indien gegevens niet meer actueel zijn, worden deze aangevuld met de meest recente informatie of, indien de bewaartermijn is verstreken, vernietigd.

10 VERSTREKKING EN TER BESCHIKKING STELLING

10.1 Uitgangspunten

Politiegegevens worden uitsluitend verstrekt aan derden indien:

- Een wettelijke grondslag voor verstrekking aanwezig is
- De verstrekking noodzakelijk is voor de uitvoering van de politietaak of voor een ander zwaarwegend algemeen belang
- De verstrekking in overeenstemming is met het doel waarvoor de gegevens zijn verzameld

10.2 Categorieën ontvangers

Het waterschap kan politiegegevens verstrekken aan de volgende categorieën ontvangers:

- Politie, Koninklijke Marechaussee en Openbaar Ministerie
- Andere opsporingsdiensten
- Bestuursorganen in het kader van hun wettelijke taken
- Andere waterschappen met boa's
- Justitiële instanties (rechtbank, rechter-commissaris)

Verstrekkingen aan andere partijen dan bovengenoemde (inclusief derde landen) zijn uitsluitend toegestaan na toestemming van de teammanager Vergunning en Handhaving en de Privacy Officer en/of Functionaris Gegevensbescherming. Deze verstrekkingen hebben tot op heden nog niet plaatsgevonden.

10.3 Procedure voor verstrekking

Bij elke verstrekking wordt vastgelegd:

- Aan wie de gegevens zijn verstrekt
- Welke gegevens zijn verstrekt
- Op welke datum de verstrekking heeft plaatsgevonden
- Op basis van welke grondslag de verstrekking is geschied
- Het doel waarvoor de verstrekking is geschied

Deze vastlegging vindt plaats door de BOA in BRS en is onderdeel van de dossiervorming.

10.4 Ter beschikking stelling

Indien politiegegevens ter beschikking worden gesteld aan derden (bijvoorbeeld bij samenwerking in een onderzoek), worden aanvullende afspraken gemaakt over:

- De duur van de ter beschikking stelling
- De doeleinden waarvoor de gegevens mogen worden gebruikt
- De beveiligingsmaatregelen bij de ontvangende partij
- De vernietiging van de gegevens na afloop

Deze afspraken worden schriftelijk vastgelegd in een samenwerkingsovereenkomst of convenant.
Bij een weigering van een beschikkingstellingsverzoek, wordt de aanvrager minimaal schriftelijk op de hoogte gesteld door de Privacy Officer.

11 BEWAARTERMIJNEN EN VERNIETIGING

11.1 Wettelijke bewaartermijnen

Voor politiegegevens gelden de bewaartermijnen zoals vastgelegd in artikel 14 van de Wpg. De belangrijkste bewaartermijnen voor het waterschap zijn:

- Dagelijkse politietaak: Politiegegevens worden bewaard voor maximaal 5 jaren na de datum van laatste verwerking, tenzij sprake is van een afwijkende bewaartermijn op grond van de aard van de gegevens of de ernst van het delict
- Specifiek onderzoek: Politiegegevens worden bewaard voor de duur van het onderzoek plus maximaal 5 jaren, tenzij de gegevens noodzakelijk blijven voor een vervolgonderzoek of strafvervolging

11.2 Periodieke controle

De bewaartermijnen worden periodiek gecontroleerd door BRS. Gegevens waarvan de bewaartermijn is verstreken worden vernietigd, tenzij sprake is van een wettelijke grond om de gegevens langer te bewaren (bijvoorbeeld lopende rechtszaak, hangende bezwaar- of beroepsprocedure).

11.3 Procedure voor vernietiging

Vernietiging van politiegegevens vindt plaats conform wetgeving en omvat definitieve verwijdering uit alle systemen en back-ups.
Uitzondering: Gegevens kunnen worden geanonimiseerd en bewaard voor statistische of wetenschappelijke doeleinden, mits herleiding tot individuele personen niet meer mogelijk is.

11.4 Archiefwet

Voor zover van toepassing worden politiegegevens die blijvende waarde hebben overgedragen aan het archief conform de Archiefwet, de Selectielijst Waterschappen en de gemeenschappelijke regeling van het waterschap. Dit betreft met name gegevens van historisch belang.

12 RECHTEN VAN BETROKKENEN

12.1 Informatieplicht

Het waterschap informeert betrokkenen over de verwerking van hun politiegegevens door middel van een privacyverklaring die beschikbaar is op de website van het waterschap Noorderzijlvest.
De privacyverklaring bevat minimaal informatie over:

- De identiteit van de verwerkingsverantwoordelijke
- De doeleinden van de verwerking
- De rechtsgrond voor de verwerking

- De categorieën gegevens die worden verwerkt
- De bewaartermijnen
- De rechten van betrokkenen
- De contactgegevens van de FG
- De mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens

12.2 Recht op inzage
Betrokkenen hebben het recht om inzage te krijgen in hun politiegegevens, tenzij sprake is van een wettelijke grond om inzage te weigeren (bijvoorbeeld indien inzage het opsporingsbelang schaadt of de privacy van derden aantast).
Verzoeken om inzage worden behandeld door Privacy Officer in samenwerking met de FG. Het waterschap beslist conform de procedure Rechten van betrokkenen op het verzoek. Een verzoek kan worden ingediend via privacy@noorderzijlvest.nl.

12.3 Recht op correctie, aanvulling en verwijdering
Betrokkenen kunnen verzoeken om correctie van onjuiste gegevens, aanvulling van onvolledige gegevens of verwijdering van gegevens die onrechtmatig zijn verwerkt.
Het waterschap beoordeelt elk verzoek op basis van de wettelijke criteria en beslist conform de procedure Rechten van betrokkenen of het verzoek wordt ingewilligd. Indien het verzoek wordt toegewezen, worden de betreffende gegevens gecorrigeerd, aangevuld of verwijderd en ontvangt de betrokkene een bevestiging.

12.4 Motivering bij afwijzing
Indien een verzoek tot inzage, correctie of verwijdering wordt afgewezen, ontvangt de betrokkene een schriftelijke en gemotiveerde beslissing waarin de reden voor afwijzing en de mogelijkheid tot bezwaar worden toegelicht.

12.5 Klachtprocedure
Betrokkenen die een klacht hebben over de verwerking van hun politiegegevens kunnen contact opnemen met de FG, via privacy@noorderzijlvest.nl. Daarnaast kunnen zij een klacht indienen bij de Autoriteit Persoonsgegevens.

13 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

13.1 Wettelijke verplichting
Het waterschap is verplicht om een DPIA uit te voeren wanneer een (nieuwe of gewijzigde) verwerking van politiegegevens waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van betrokkenen.
Een DPIA is voor het gebruik van BRS en politiegegevens verplicht door:
- Gebruik van nieuwe technologieën voor de verwerking van politiegegevens
- Verwerking van locatiegegevens
- Verwerking van persoonsgegevens over kwetsbare groepen of personen
- Grootschalige verwerking van bijzondere categorieën politiegegevens
- Systematische observatie van openbare ruimten op grote schaal
- Geautomatiseerde besluitvorming met rechtsgevolgen of vergelijkbare significante effecten
- Vergelijking of koppeling van datasets uit verschillende bronnen

13.2 Procedure voor uitvoering
Voorafgaand aan de implementatie van een nieuwe of gewijzigde verwerking beoordeelt de Privacy Officer in samenspraak met de FG of een DPIA vereist is. Indien dit het geval is, wordt een DPIA uitgevoerd conform het Stappenplan DPIA.
De DPIA bevat minimaal:
- Een systematische beschrijving van de beoogde verwerking en de doeleinden daarvan
- Een beoordeling van de noodzakelijkheid en proportionaliteit van de verwerking
- Een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen
- De voorgenomen maatregelen om de risico's aan te pakken

13.3 Rol van de FG en extern advies
De FG wordt betrokken bij de uitvoering van de DPIA en geeft advies over de proportionaliteit van de verwerking en de toereikendheid van de beveiligingsmaatregelen.

Indien de DPIA uitwijst dat de verwerking een hoog risico oplevert dat niet adequaat kan worden beperkt, overlegt het waterschap met de Autoriteit Persoonsgegevens voordat de verwerking wordt gestart.

13.4 Documentatie en herziening
Alle uitgevoerde DPIA's worden gedocumenteerd en bewaard in het Information Security Management Systeem (ISMS). DPIA's worden herzien wanneer zich relevante wijzigingen voordoen in de verwerking of in de risico's of zodra de DPIA 3 jaren oud is.

14 DATALEKKEN

14.1 Definitie datalek
Een datalek is een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of ongeoorloofde toegang tot politiegegevens.
Voorbeelden van datalekken:
- Verlies van laptop, USB-stick of papieren dossier met politiegegevens
- Versturen van gegevens naar verkeerde ontvanger
- Hacken of phishing waarbij politiegegevens zijn gecompromitteerd
- Onbevoegde toegang door (voormalige) medewerkers
- Ransomware of andere malware die toegang tot gegevens belemmert

14.2 Meldplicht
Op grond van artikel 33a Wpg is het waterschap verplicht om een datalek te melden aan de Autoriteit Persoonsgegevens wanneer het datalek waarschijnlijk een risico inhoudt voor de rechten en vrijheden van betrokkenen.
Daarnaast moet het waterschap de betrokkene(n) informeren wanneer het datalek waarschijnlijk een hoog risico inhoudt voor hun rechten en vrijheden, tenzij dit de opsporing zou schaden of onevenredige inspanning zou vergen.

14.3 Meldprocedure
Elke medewerker die een (vermoeden van een) datalek constateert, meldt dit onmiddellijk in Topdesk. Het meldpunt beoordeelt of sprake is van een meldplichtig datalek. Indien dit het geval is, wordt de melding binnen 72 uur na constatering gedaan aan de Autoriteit Persoonsgegevens conform de Procedure Datalekken.

14.4 Registratie en evaluatie
Alle datalekken, ook niet-meldplichtige, worden geregistreerd in het datalekkenregister. Dit register bevat minimaal:
- Datum en tijdstip van constatering
- Aard en omvang van het datalek
- Betrokken categorieën gegevens en aantal betrokkenen
- Genomen maatregelen om het lek te verhelpen
- Eventuele melding aan Autoriteit Persoonsgegevens en betrokkenen

Na afhandeling van het datalek wordt een evaluatie uitgevoerd om herhaling te voorkomen. De uitkomsten worden besproken met het management en vertaald naar verbetermaatregelen.

15 VERWERKERS EN DERDEN

15.1 Verwerkersovereenkomsten
Indien het waterschap gebruikmaakt van externe partijen die in opdracht van het waterschap politiegegevens verwerken (bijvoorbeeld ICT-leveranciers, hosting-providers), wordt met deze partijen een verwerkersovereenkomst gesloten conform artikel 6c Wpg.
De verwerkersovereenkomst bevat minimaal:
- Het onderwerp, de duur, de aard en het doel van de verwerking
- De soorten politiegegevens en categorieën betrokkenen
- De verplichtingen en rechten van de verwerkingsverantwoordelijke
- De instructies van de verwerkingsverantwoordelijke aan de verwerker
- De verplichting tot geheimhouding
- De beveiligingsmaatregelen die de verwerker moet treffen
- De voorwaarden voor inschakeling van subverwerkers
- De bijstand aan de verwerkingsverantwoordelijke bij uitoefening van rechten door betrokkenen
- De verplichtingen bij beëindiging van de verwerking

15.2 Selectie en beoordeling van verwerkers
Bij de selectie van verwerkers beoordeelt het waterschap of de verwerker voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen. Deze beoordeling wordt gedocumenteerd.
Bestaande verwerkers worden minimaal jaarlijks beoordeeld op naleving van de verwerkersovereenkomst en de beveiligingsmaatregelen.

15.3 Register van verwerkers
Het waterschap houdt een actueel register bij van alle verwerkers die politiegegevens verwerken. Dit register bevat:
- Naam en contactgegevens van de verwerker
- Beschrijving van de verwerkingsactiviteiten
- Datum van afsluiten verwerkersovereenkomst
- Beoordelingsdatum en uitkomsten

16 BEWUSTWORDING EN TRAINING

16.1 Verplichte training voor boa's
Elke boa doorloopt bij indiensttreding verplicht een Wpg-training waarin aandacht wordt besteed aan:
- De wettelijke kaders van de Wpg
- De principes van rechtmatige verwerking
- De noodzakelijkheidstoets
- Omgang met bijzondere categorieën politiegegevens
- Rechten van betrokkenen
- Beveiliging en geheimhouding
- Meldplicht datalekken

Deelname aan de training wordt vastgelegd in het personeelsdossier.
Aanvullend is geborgd dat de boa of een andere persoon aan wie politiegegevens ter beschikking zijn gesteld formeel bekend is met de plicht tot geheimhouding en de consequenties bij schending van deze plicht. Dit is uitbesteed aan NatuurNetwerk.
Voordat boa’s gebruik mogen maken van BRS, stelt NatuurNetwerk vast dat zij beschikken over een aanstellingsakte en dat zij zijn beëdigd door de Korpschef met opsporingsbevoegdheid. Hierbij worden de boa’s formeel bekend gemaakt met de plicht tot geheimhouding en de consequenties bij schending van deze plicht. NatuurNetwerk maakt de gebruikers in de gebruikersovereenkomst formeel bekend met de plicht tot geheimhouding en de consequenties bij schending van deze plicht.

16.2 Periodieke bijscholing
Alle boa's en andere medewerkers die betrokken zijn bij de verwerking van politiegegevens doorlopen via NatuurNetwerk minimaal jaarlijks een opfriscursus of bijscholing over de Wpg en relevante ontwikkelingen.

16.3 Bewustwordingscampagnes
Het waterschap organiseert periodiek bewustwordingscampagnes gericht op privacy en gegevensbescherming. Deze campagnes zijn gericht op:
- Het vergroten van bewustzijn bij alle medewerkers
- Het bespreekbaar maken van privacy-dilemma's
- Het delen van best practices en leerervaringen

Verantwoordelijke voor training en bewustwording: Privacy Officer

17 INTERNE EN EXTERNE AUDITS

17.1 Interne audits
Het waterschap voert jaarlijks interne audits uit op de naleving van de Wpg. Deze audits richten zich op:
- De opzet en het bestaan van maatregelen en procedures
- De werking van de getroffen maatregelen en procedures
- De naleving van dit beleid door medewerkers
- De actualiteit van het register van verwerkingen
- De beveiliging van systemen en gegevens

De interne audits worden uitgevoerd volgens een vastgesteld auditplan. De resultaten worden gerapporteerd aan het Dagelijks Bestuur door de Teammanager Vergunning en Handhaving.

17.2 Externe privacy audit

Op grond van artikel 33 Wpg laat het waterschap minimaal eens per vier jaren een externe privacy audit uitvoeren door een onafhankelijke en gekwalificeerde auditor conform het controleprotocol van NOREA. De externe audit richt zich op alle aspecten van de Wpg-naleving, waaronder:

- Principes en rechtmatigheid
- Gegevensbescherming
- Autorisaties en toegangsbeheer
- Verwerkers en terbeschikkingstelling
- Informatiebeveiliging
- Bewaartermijnen en vernietiging
- Register en documentatie
- Datalekken
- DPIA's
- Logging en monitoring

17.3 Auditrapportage en opvolging

De externe auditor stelt een auditrapport en een controleverklaring op. Deze documenten worden aangeboden aan het bestuur en bewaard conform de wettelijke vereisten. Het auditrapport is opvraagbaar door de Autoriteit Persoonsgegevens.
Geconstateerde bevindingen en aanbevelingen uit interne en externe audits worden vertaald naar een verbeterplan met concrete acties en termijnen. De uitvoering van het verbeterplan wordt gemonitord door de verantwoordelijk manager Toezicht en Handhaving en de Functionaris Gegevensbescherming.

18 TOEZICHT EN VERANTWOORDING

18.1 Interne verantwoording

Het dagelijks bestuur ontvangt minimaal jaarlijks een rapportage over de naleving van de Wpg binnen het waterschap. Deze rapportage bevat minimaal:

- Een overzicht van verwerkingsactiviteiten
- Resultaten van interne audits
- Overzicht van datalekken en getroffen maatregelen
- Uitgevoerde DPIA's
- Aantal verzoeken van betrokkenen en afhandeling
- Wijzigingen in verwerkingen of systemen
- Geplande verbeteracties

Verantwoordelijke voor jaarrapportage: Functionaris Gegevensbescherming

18.2 Externe verantwoording

Het waterschap verstrekt op verzoek van de Autoriteit Persoonsgegevens of het Ministerie van Justitie en Veiligheid alle benodigde informatie en toegang tot systemen en documentatie om naleving van de Wpg te kunnen toetsen.

18.3 Transparantie naar burgers

Het waterschap maakt de privacyverklaring (welke eveneens toeziet op de Wpg) en andere relevante informatie over de verwerking van politiegegevens openbaar toegankelijk via de website van het waterschap.

19 INCIDENTENBEHEER EN ESCALATIE

19.1 Incidentenregistratie

Naast datalekken worden ook andere beveiligingsincidenten en privacyschendingen geregistreerd, zoals:

- Onbevoegde toegang tot systemen (zonder dat sprake is van een datalek)
- Pogingen tot inbraak of hacken
- Misbruik van autorisaties door medewerkers
- Verlies van toegangssleutels of inloggegevens

Deze incidenten worden gemeld en geregistreerd in het incidentenregister.

19.2 Escalatieprocedure
Afhankelijk van de ernst van het incident wordt een escalatieprocedure gevolgd conform de Procedure datalekken.

19.3 Maatregelen bij overtreding
Bij overtreding van dit beleid of de Wpg door medewerkers kunnen de volgende maatregelen worden genomen:
- Intrekking van autorisaties
- Herhalingstraining
- Formele waarschuwing
- Disciplinaire maatregelen
- Ontslagprocedure (bij ernstige of herhaalde overtredingen)
- Strafrechtelijke aangifte (bij opzettelijk misbruik)

20 EVALUATIE EN ACTUALISATIE VAN BELEID

20.1 Periodieke evaluatie
Dit beleid wordt minimaal eens per 4 jaren geëvalueerd op actualiteit en effectiviteit. De evaluatie wordt uitgevoerd door de teammanager Vergunning en Handhaving in samenwerking met de FG.
Bij de evaluatie worden betrokken:
- Resultaten van interne en externe audits
- Wijzigingen in wet- en regelgeving
- Geconstateerde knelpunten in de praktijk
- Nieuwe technologische ontwikkelingen
- Feedback van medewerkers en betrokkenen

20.2 Actualisatie
Op basis van de evaluatie wordt beoordeeld of actualisatie van dit beleid noodzakelijk is. Actualisatie vindt in ieder geval plaats bij:
- Wijziging van de Wpg of andere relevante wet- en regelgeving
- Ingrijpende organisatiewijzigingen
- Implementatie van nieuwe systemen of technologieën
- Wijziging van taken of bevoegdheden van boa's
- Geconstateerde ernstige tekortkomingen

Geactualiseerd beleid wordt ter vaststelling voorgelegd aan het dagelijks bestuur en na vaststelling gecommuniceerd naar alle betrokken medewerkers.

20.3 Communicatie van wijzigingen
Bij wijziging van dit beleid wordt dit gecommuniceerd via:
- Publicatie op Waterweb
- E-mailbericht aan alle betrokken medewerkers
- Bespreking in teamoverleggen
- Bijscholing indien noodzakelijk

Bij de evaluatie worden betrokken:
- Resultaten van interne en externe audits
- Wijzigingen in wet- en regelgeving
- Geconstateerde knelpunten in de praktijk
- Nieuwe technologische ontwikkelingen
- Feedback van medewerkers en betrokkenen

21 SLOTBEPALINGEN

21.1 Inwerkingtreding
Dit beleid treedt in werking op 8 september 2026.

21.2 Citeertitel
Dit beleid kan worden aangehaald als: "Beleid Wet politiegegevens (Wpg) waterschap Noorderzijlvest".

21.3 Vaststellingsbesluit

Dit beleid is vastgesteld door het dagelijks bestuur op 8 september 2026.

22 GELIEERDE DOCUMENTEN

De volgende documenten maken integraal onderdeel uit van dit beleid:

1. Autorisatiematrix
2. Verwerkingsregister
3. Privacyverklaring
4. Procedure datalekken
5. Stappenplan DPIA
6. Procedure Rechten van betrokkenen

Januari 2026