

Beleid Wet politiegegevens Waterschap Vechtstromen

Het dagelijks bestuur van waterschap Vechtstromen;

gezien het advies d.d. 15 juni 2026;

gelet op de artikelen 56 en 77 van de Waterschapswet;

BESLUIT

1. het geactualiseerde beleid Wet politiegegevens Waterschap Vechtstromen vast te stellen;
2. de aanbevelingen uit de interne audit Wet politiegegevens te implementeren overeenkomstig het verbeterplan; en
3. het bestaande beleid Wet politiegegevens in te trekken met ingang van de datum van inwerking-treding van het geactualiseerde beleid.

1. Inleiding

1.1 Voorwoord

Privacy is een Grondrecht. Privacy is een voorwaarde om vrij te zijn in wie je bent en wat je doet. De Algemene Verordening Gegevensbescherming (AVG) handelt over informationele Privacy. Hiervoor is een Privacy beleid opgesteld. De verwerking van politiegegevens door buitengewoon opsporingsambtenaren (boa's) valt echter niet alleen onder de AVG maar ook onder de Wet politiegegevens (Wpg).

Daarnaast is een aantal andere regelingen van toepassing op de verwerking van politiegegevens. Zoals het Besluit politiegegevens (Bpg), het Besluit politiegegevens buitengewoon opsporingsambtenaren en de Regeling periodieke audit politiegegevens. Deze wetten en regelgevingen kennen op enkele gebieden wat onderlinge verschillen.

Zo kent de Wpg bijvoorbeeld specifieke bewaartermijnen voor de opslag van politiegegevens, terwijl de AVG geen concrete bewaartermijnen voorschrijft. Ook stelt de Wpg andere eisen bij het delen van politiegegevens tussen verschillende partijen, is er een verplichting tot logging en zijn er in de Wpg aanvullende beperkingen en uitzonderingen op de in de AVG geldende privacyrechten van betrokkenen. Andere verplichtingen zijn vergelijkbaar maar kennen verschillen in de concrete uitwerking, zoals de verplichting voor de verwerkingsverantwoordelijke om passende technische en organisatorische maatregelen te treffen ter bescherming en beveiliging van de gegevens.

Het huidige Privacybeleid van het waterschap Vechtstromen gaat alleen uit van de AVG. Er is voor gekozen de verplichtingen uit de Wpg in een apart Wpg beleid te beschrijven. Bij dit beleid hoort een Wpg-reglement waarin de verplichtingen uit de Wpg voor Vechtstromen artikelsgewijs staan beschreven. Dit reglement is in een apart beleidsstuk opgenomen.

1.2 Visie op Privacy

Als overheidsorganisatie heeft onze organisatie wettelijke taken waarvoor het noodzakelijk is om persoonsgegevens en politiegegevens te verwerken. Uitgangspunt is dat het voor de medewerkers van onze organisatie vanzelfsprekend is om zorgvuldig met deze gegevens om te gaan. Vechtstromen wil worden ervaren als een verbindende, maatschappelijk betrokken organisatie. Betrouwbaar zijn is daar onlosmakelijk mee verbonden.

Het voorkomen van boetes van de Autoriteit Persoonsgegevens (AP) is daarom niet de directe reden om zorgvuldig met politiegegevens om te gaan; de medewerkers van Vechtstromen zijn intrinsiek gemotiveerd om de informationele Privacy van betrokkenen te respecteren en zien vanuit die gedachte de wetgeving als een hulpmiddel hierin. Dit geldt zowel voor het gebruik van persoonsgegevens onder de AVG als het gebruik van politiegegevens onder de Wpg.

Privacy is van ons allemaal

Een Wpg beleid geeft onze organisatie houvast en richting voor het verwerken van politiegegevens in het dagelijks gebruik. We staan een pragmatische, maar (juridisch) correcte, toepassing van de wettelijke kaders voor. En we kijken daarbij vooral naar de voorwaarden om politiegegevens te kunnen verwerken, in plaats van de beperkingen.

Vechtstromen laat hiermee zien dat inwoners, agrariërs, ondernemers, medewerkers en andere betrokkenen die met ons waterschap te maken hebben, kunnen vertrouwen op voldoende bescherming van hun Privacy.

Met dit beleid willen we onder andere bereiken dat de boa's van Vechtstromen:

- 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.

1.3 Doelen

Met het voorliggend Wpg beleid beoogt onze organisatie het volgende:

- Het stimuleren en borgen van een betrouwbare organisatie en imago.
- Onze organisatie kaders en richtlijnen geven voor het verwerken van politiegegevens in de dagelijkse procesgang.
- Het waarborgen van het zorgvuldig omgaan met politiegegevens, conform de wet- en regelgeving.

1.4 Doelgroepen

Het Wpg beleid is bedoeld voor de buitengewoon opsporingsambtenaren (BOA's) en de Bevoegd Functionaris (BF) die namens Waterschap Vechtstromen politiegegevens verwerken.

1.5 Reikwijdte Wpg beleid

Het Wpg beleid is van toepassing op de gehele organisatie, alle taken en processen, objecten, gegevensverzamelingen en onderliggende informatiesystemen waar Vechtstromen verantwoordelijk voor is die worden gebruikt ter uitvoering van de taken van de buitengewoon opsporingsambtenaren (BOA's) die vallen onder de Wet politiegegevens (Wpg).

Het Wpg beleid van Vechtstromen heeft op het gebied van verwerking van politiegegevens een koppeling met het Privacybeleid AVG, maar is wegens de afwijkende regelgeving, ondergebracht in een separaat beleid. De teamleider Vergunningen, Toezicht en Handhaving is verantwoordelijk voor de uitvoering van het Wpg beleid en gemandateerd voor het nemen van besluiten op grond van de Wpg, voor het Wpg beleid en daaruit volgende instructies.

1.6 Leeswijzer

Het Wpg beleid is als volgt opgebouwd.

Hoofdstuk 2, 'Wpg wettelijk kader', beschrijft het wettelijk kader dat als uitgangspunt geldt voor de verwerking van de politiegegevens

Hoofdstuk 3, 'Organisatorische kader', beschrijft de rollen, taken en verantwoordelijkheden binnen Vechtstromen op het gebied van de Wpg,

Hoofdstuk 4, 'Basisbeginselen verwerking politiegegevens', beschrijft de basisbeginselen die gelden bij de verwerking van politiegegevens.

In hoofdstuk 5, 'Verwerkingsregister Wpg', wordt het Verwerkingsregister Wpg toegelicht.

Hoofdstuk 6, 'Het ter beschikking stellen en verstrekken van politiegegevens', licht toe welke regels er gelden voor het delen van politiegegevens.

Hoofdstuk 7, 'Het bewaren van politiegegevens', licht toe welke regels er gelden voor het bewaren van politiegegevens.

Hoofdstuk 8, 'Datalekken', schetst de afwijkende regelgeving die van toepassing is in geval van een datalek onder de Wpg.

Hoofdstuk 9, 'Privacy door ontwerp en Privacy door standaardinstellingen', geeft een beschrijving van de concepten van privacy by design/default.

Hoofdstuk 10, 'Data protection impact assessment', geeft een beschrijving van de data protection impact assessment.

Hoofdstuk 11, 'Audits', geeft een beschrijving van de verplichte audits onder de Wpg.

Hoofdstuk 12, 'Review beleid', geeft een beschrijving van de periodieke review van dit Wpg-beleid.

In de bijlage 1 is een verklarende woordenlijst opgenomen met specifieke AVG en Wpg-begrippen die in dit Wpg beleid zijn opgenomen.

2. Wpg wettelijke kader

Het wettelijke kader van de Wpg is voor een deel gelijklopend aan dat van de AVG. Op hoofdlijnen geldt aanvullend nog het volgende:

- 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 politiegegevens dan de AVG. Zo geldt onder andere de plicht tot delen met ieder andere opsporingsambtenaar die deze gegevens nodig heeft voor zijn werk.

De hierna genoemde verplichtingen uit de Wpg zijn geborgd binnen onze applicaties (met name in het Boa Registratie Systeem, BRS):

- Er moet een scheiding worden aangebracht tussen gegevens die op feiten zijn gebaseerd en feiten die op een persoonlijk oordeel zijn gebaseerd;
- Er moet onderscheid worden gemaakt tussen betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden;
- Documentatie is vereist van de doelen van onderzoeken, verstrekking of doorgifte, afwijzing van verzoeken om inzage, inbreuk op de beveiliging, doorgifte buiten de EU met datum en tijd, ontvanger, redenen en doorgegeven gegevens en melding van gemeenschappelijke verwerkingen aan de Autoriteit Politiegegevens (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 (art. 32a Wpg).
- Er worden specifieke eisen gesteld aan de informatiebeveiliging in het Besluit politiegegevens (Bpg)

3. Organisatorisch kader

Het verwerken van politiegegevens is geen kernactiviteit van waterschap Vechtstromen, maar wel een afgeleide van of ondersteunend aan de primaire processen. Binnen Vechtstromen zijn er verschillende rollen, functies en overlegorganen met bijbehorende taken op het gebied van de Wpg.

Dagelijks bestuur (DB)

Als verwerkingsverantwoordelijke is het dagelijks bestuur ten aanzien van verwerkingen van politiegegevens door boa's verantwoordelijk voor:

- Een correcte reactie op uitoefening van de rechten van betrokkenen
- Het bijhouden van een register van verwerkingen
- Melding en optreden bij datalekken
- Het sluiten van verwerkersovereenkomsten.

Het DB is daarnaast, in het kader van de zorg voor de dagelijkse gang van zaken, verantwoordelijk voor de correcte implementatie en naleving en Wpg.

Portefeuillehouder van DB

Wpg kwesties vallen onder de Portefeuillehouder VTH. Deze portefeuillehouder is daarmee het bestuurlijk aanspreekpunt voor Wpg kwesties.

Functionaris Gegevensbescherming (FG)

Net als de AVG verplicht artikel 36 van de Wpg tot het aanstellen van de FG. De taak van de FG is om toezicht te houden op de naleving van de Wpg binnen Vechtstromen. Hij rapporteert hierover rechtstreeks aan het DB. De FG houdt voor wat betreft de naleving van de Wpg binnen Vechtstromen toezicht op de volgende elementen:

- Doelbinding t.a.v. het gebruiken van politiegegevens door Vechtstromen.
- Noodzakelijkheid, rechtmatigheid en herkomst van gegevens,
- Het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van de persoonsgegevens,
- de toewijzing van de autorisaties, bedoeld in art. 6,
- de bewustmaking en opleiding van de boa's betrokken bij de verwerking van politiegegevens,

- de audits,
- de uitvoering van de DPIA's.

De FG wordt door de verwerkingsverantwoordelijke tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van politiegegevens. De FG stelt jaarlijks een verslag op van zijn bevindingen en stelt dit ter beschikking aan de verwerkingsverantwoordelijke.

De FG is de contactpersoon met de Autoriteit Persoonsgegevens voor aangelegenheden die verband houden met verwerking van persoonsgegevens en politiegegevens

Daarnaast adviseert en informeert de FG de verschillende onderdelen van de organisatie over de uitvoering van de AVG en Wpg. Hierbij kiest de FG voor een balans tussen het bevorderen van de bewustzijn en het bewaken van de naleving van wet- en regelgeving.

De FG heeft een, wettelijk bepaalde, onafhankelijke functie. Dit betreft idealiter een staffunctie onder de Secretaris-Directeur. Omdat Vechtstromen in haar organogram niet in een dergelijke functie voorziet, is de FG vooralsnog organisatorisch ondergebracht bij het team FJI.

Privacy Officer Wpg

De Privacy Officer rapporteert aan de teamleider VTH en werkt nauw samen met de Functionaris Gegevensbescherming. Bij afwezigheid van de FG verzorgt de Privacy Officer, indien noodzakelijk, de contacten met de Autoriteit Politiegegevens en vervangt de Functionaris Gegevensbescherming zo nodig in vergaderingen.

De Privacy Officer is het eerste aanspreekpunt bij Privacy vragen van collega's en betrokkenen en ondersteunt en adviseert het management bij de uitvoering van het Privacybeleid en bewustwordingsactiviteiten. Tevens voert de Privacy Officer beleidsmatige taken uit, zoals het actueel houden van het Privacybeleid, integrale Privacy procedures en richtlijnen. Dit geldt zowel voor taken vanuit de AVG alsmede voor taken i.h.k.v. de Wpg.

Directieteam

Als hoogste ambtelijke leiding is het directieteam verantwoordelijk voor de prestaties van de organisatie. Ten aanzien van de AVG en Wpg stuurt het directieteam op de implementatie en naleving van de AVG/Wpg. Dit vindt in ieder geval plaats via sturing op de Concern A3, de daarvan afgeleide teamplannen en halfjaarlijkse bilateralen met de FG.

Binnen het directieteam is de Secretaris-directeur het aanspreekpunt voor Wpg kwesties.

Teamleider Vergunningen, Toezicht en Handhaving (VTH)

Op basis van de ondermandatering is de Teamleider VTH bevoegd om namens het DB te besluiten op verzoeken van betrokkenen in het kader van de Wpg. Daarnaast is ook de verdere uitvoering van de Wpg belegd bij de Teamleider VTH.¹ Dit uit zich in de volgende verantwoordelijkheden:

- Fungeert als aanspreekpunt voor AVG m.b.t. VTH-dossiers, voor het DT, de SD en het DB.
- Actualiseert het verwerkingsregister Wpg.
- Reageert namens het DB (in ondermandaat) op verzoeken van betrokkene op basis van de Wpg.
- Is verantwoordelijk voor het opstellen en actualiseren van integrale richtlijnen.

Op basis van de ondervolmacht is de teamleider VTH bevoegd om namens het DB, verwerkersovereenkomsten, i.h.k.v. de Wpg, te sluiten.

De teamleider VTH is in het kader van algemene zorg voor de naleving van geldende wetgeving verantwoordelijk voor:

- Het stimuleren en borgen van Wpg procesafspraken en Wpg gerelateerde maatregelen vanuit projecten of vraagstukken.
- De inhoud, volledigheid en het actueel zijn van de verwerkingen van politiegegevens binnen het eigen team in het Wpg verwerkingsregister
- De aanwezigheid van contractuele afspraken (verwerkersovereenkomsten) met externe partijen die politiegegevens verwerken.
- Het informeren van de medewerkers over actualiteiten en zorgdragen voor blijvende bewustwording met ondersteuning van de Privacy Officer, de Privacydesk en/of FG.
- Het sturen op verbeteracties van het eigen team naar aanleiding van een datalek, Wpg-audit en/of adviezen van de Privacy Officer en de FG.

1) Conform de ondermantering met betrekking tot AVG bevoegdheden.

- Het laten uitvoeren van een DPIA ter beoordeling van risico's bij nieuwe en/of gewijzigde applicaties of processen.

Securityboard

Binnen Vechtstromen is een Securityboard ingesteld. Een overlegorgaan met als doel om de organisatiedoelstellingen voor informatieveiligheid zoals gedefinieerd in het Strategisch Informatiebeleid te bereiken.

De FG maakt deel uit van dit overlegorgaan vanuit diens rollen om toezicht te houden op en advies te geven over de verwerking van persoons en politiegegevens en naleving van de AVG en de Wpg, met name gericht op het integriteit- en vertrouwelijkheidsbeginsel (zie ook hoofdstuk 3). Ook biedt het de gelegenheid voor de FG om in directe aanwezigheid van het verantwoordelijke directielid te informeren en te escaleren over Privacy risico's. Daarnaast brengt de FG in de Securityboard verslag uit over voorgenomen en gehouden Wpg-audits.

De Bevoegd Functionaris (BF)

De medewerker Handhaving/BOA-Coördinator is verantwoordelijk voor het uitvoeren van de taak bevoegd functionaris. Dit is de 'hoeder' van de gegevens die onder artikel 9 Wpg worden verwerkt. Deze functionaris is beschreven in artikel 2:10, eerste lid, van het Bpg. Het moet een persoon zijn met voldoende kennis en vaardigheden over dit type gegevens. Deze functionaris beslist bijvoorbeeld wie er toegang mag hebben tot deze gegevens en of ze verstrekt kunnen worden aan een samenwerkingspartner. Iedere artikel 9-verwerking dient een BF te hebben. De BF heeft onder andere de volgende taken:

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

Medewerkers BOA's en Bevoegd Functionaris

Het zorgvuldig omgaan met politiegegevens is voor een belangrijk deel afhankelijk van het Privacy bewustzijn, in denken en doen, van de BOA's en andere WPG functionarissen van Waterschap Vechtstromen.

De BOA's en Bevoegd Functionaris zijn verantwoordelijk voor:

- Het volgens de vereisten van de Wpg verwerken van politiegegevens.
- Het zich bewust zijn van de rechten van betrokkenen en er naar handelen.
- Het melden van verwerkingen ten behoeve van het verwerkingsregister Wpg.
- Het melden van (vermoedelijke) datalekken.
- Het zich bewust zijn van geheimhouding en verbod op profilering.

4. Basisbeginselen verwerking politiegegevens

In dit Wpg beleid worden de kaders voor het omgaan met politiegegevens vastgelegd. Waterschap Vechtstromen hanteert, conform de AVG en Wpg, de zes basisbeginselen bij de verwerking van politiegegevens.² Indien er bijvoorbeeld sprake is van de mogelijke implementatie van een nieuwe applicatie of er een samenwerking met een derde partij wordt overwogen waarbij politiegegevens worden verwerkt, is de beoordeling van de basisbeginselen een van de randvoorwaarden in de besluitvorming. We hanteren deze basisbeginselen als 'kapstok' voor het Wpg beleid.

- Rechtmatig, behoorlijk en transparant**
Wij zorgen ervoor dat er een rechtsgrond is voor de verwerking van politiegegevens van een betrokkene (zijnde inwoners, agrariërs, ondernemers, medewerkers en andere betrokkenen die met ons waterschap te maken hebben).
- Doelbinding**
Voordat we met de verwerking van politiegegevens van een betrokkene beginnen, wordt gecontroleerd dat het doel van de verwerking is vastgelegd.
- Minimale gegevensverwerking**
Vechtstromen verwerkt niet meer politiegegevens dan strikt noodzakelijk is voor het doel dat vooraf is geformuleerd. Overbodige politiegegevens worden zo snel mogelijk gewist en/of niet opgevraagd.
- Juistheidsbeginsel**
We hebben een inspanningsplicht om ervoor te zorgen dat de politiegegevens van betrokkenen die we verwerken juist, volledig en actueel zijn.
- Opslagbeperking**

2) Conform art. 5 van de AVG

- We bewaren politiegegevens niet langer dan strikt noodzakelijk is.
- f. **Integriteit- en vertrouwelijkheid**
Vechtstromen treft passende technische en organisatorische maatregelen om ongeoorloofde toegang tot politiegegevens te voorkomen. Denk aan cryptografie, juiste autorisaties en sterke wachtwoorden. Deze maatregelen zijn ondervangen door het gebruik van het Boa Registratie Systeem (BRS). Tevens is het Strategisch Informatieveiligheidsbeleid 2.0 van toepassing op het verwerken van politiegegevens.
- g. **Doorgifte buiten de EU**
Vechtstromen verstrekt geen politiegegevens aan organisaties die zich bevinden in derde landen buiten de EU.

5. Verwerkingsregister Wpg

De Wpg verplicht tot het bijhouden van een register van verwerkingen. Wel zijn er enkele verschillen met het register dat wordt opgesteld op basis van de AVG. Deze verschillen zijn hierna met een (*) 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 politiegegevens;
- 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. (*)

Om te borgen dat de gegevensverwerkingen geregistreerd worden, heeft het waterschap concrete werkafspraken vastgesteld. Binnen Vechtstromen vinden geen verwerkingen plaats als bedoeld in artikel 13 van de Wet politiegegevens. De verwerking van politiegegevens blijft beperkt tot de in dit beleid en het verwerkingsregister opgenomen categorieën van verwerkingen. Hiermee wordt geborgd dat geen gegevens worden verwerkt buiten de vastgestelde doeleinden en wettelijke kaders.

De teamleider VTH is verantwoordelijk voor de volledigheid en actualiteit van het register van verwerkingen Wpg. De Privacy Officer ziet jaarlijks toe op de actualisatie van het register. Tussentijds vindt er actualisatie plaats bij een wijziging van verwerkingen.

6. Het ter beschikking stellen en verstrekken van politiegegevens

De Wpg maakt een onderscheid tussen het ter beschikking stellen van politiegegevens en het verstrekken ervan. Dit is beschreven in artikel 15 van de Wpg.

Een synoniem hiervoor is 'free flow of information': in principe dienen politiegegevens gedeeld te worden met ieder die de gegevens nodig heeft voor zijn 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. Middels het gebruik van het Boa Registratie Systeem (BRS) is geborgd dat wanneer gegevens verstrekt worden, er wordt voldaan aan de documentatieplicht en dat de verstrekking alleen plaatsvindt in overeenstemming met het bevoegd gezag indien dit vereist is in de wet. Het gaat dan bijvoorbeeld om verstrekkingen aan de burgemeester, een toezichthouder, een advocaat of een functionaris in het kader van de Wet bibob. Indien blijkt dat gegevens niet juist waren, moeten na correctie, die instanties worden geïnformeerd waaraan de onjuiste gegevens zijn verstrekt.

Daarnaast vindt, indien daartoe aanleiding bestaat, rechtstreekse verstrekking van politiegegevens plaats aan het Openbaar Ministerie. Deze verstrekking geschiedt binnen het kader van de strafrechtelijke handhaving en is gebaseerd op de daarvoor geldende bepalingen in de Wet politiegegevens en het Besluit politiegegevens. Ook in deze gevallen wordt geborgd dat uitsluitend gegevens worden verstrekt

voor zover dit noodzakelijk is voor de uitoefening van de wettelijke taak van het Openbaar Ministerie en wordt voldaan aan de geldende documentatie- en verantwoordingsverplichtingen.

De wijze waarop politiegegevens ter beschikking kunnen worden gesteld dan wel verstrekt is uitgebreid beschreven in de procedure, 'Procedure: Verstrekken en ter beschikking stellen politiegegevens'.

7. 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, nadat de toepasselijke bewaartermijn is verlopen, ontoegankelijk worden gemaakt. Hierna kunnen deze gegevens nog maximaal vijf jaar worden bewaard. Daarna, of binnen deze periode van vijf jaar (afhankelijk van welke bewaartermijn geldt), dient definitieve vernietiging plaats te vinden. Indien van cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens. Er wordt dan aan de bewaareisen als genoemd in de Archiefwet voldaan.

Alle politiegegevens worden gelabeld in het BRS. Hier wordt gekozen voor artikel 8, 9 of 13 informatie. Voor elk label is de bewaartermijn conform de wettelijke bepaling geconfigureerd, zodat geborgd wordt dat deze politiegegevens niet langer worden bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. De wijze waarop politiegegevens worden bewaard is uitgebreid beschreven in de procedure, 'Procedure: Verwijderen, vernietigen en archivering van politiegegevens'.

8. Datalekken

In de procedure 'informatieveiligheidsincidenten en datalekken' staat beschreven op welke wijze Vechtstromen beveiligingsincidenten en datalekken behandelt conform AVG. Deze procedure is overeenkomstig van toepassing op beveiligingsincidenten met politiegegevens (datalekken).

Onder de Wpg gelden uitzonderingen m.b.t. de mededelingsplicht in geval van een datalek. Deze staan hieronder beschreven.

Op deze mededelingsplicht zijn enkele uitzonderingen van toepassing. Bijvoorbeeld als de mededeling achterwege moet blijven ter vermindering van belemmering van 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.

9. Privacy door ontwerp en Privacy door standaardinstellingen

Vechtstromen werkt volgens de principes Privacy door ontwerp en Privacy door standaardinstellingen.

Bij Privacy door ontwerp (Privacy by design) wordt meteen bij de start van het ontwerpen en/of inkoop van een product of dienst rekening gehouden met de Privacy van betrokkenen. Het doel is om de bescherming van politiegegevens aan de voorkant in te bouwen, bij bijvoorbeeld het aangaan van contracten of de start van projecten, en niet tijdens of na afloop van processen. De privacyaspecten zijn daarmee integraal onderdeel van de procesgang bij nieuwe en of gewijzigde applicaties en diensten.

In het kader van privacy door ontwerp is binnen de systemen die Vechtstromen gebruikt voor de verwerking van politiegegevens geen functionaliteit aanwezig voor het geautomatiseerd vergelijken of koppelen van gegevensbestanden. Dit geldt zowel voor de gebruikte verwerkingssystemen als voor het Boa Registratie Systeem (BRS). Hiermee wordt geborgd dat geen verdergaande gegevensverwerking plaatsvindt dan noodzakelijk, in lijn met de uitgangspunten van de Wet politiegegevens.

Privacy door standaardinstellingen (Privacy by default) is een onderdeel van Privacy door ontwerp, waarbij als uitgangspunt geldt dat de standaardinstellingen altijd zo Privacy-vriendelijk mogelijk zijn. Daardoor worden alleen die politiegegevens verwerkt die noodzakelijk zijn voor het specifieke doel.

10. Data protection impact assessment

Een data protection impact assessment (DPIA) houdt in dat voorafgaand aan een gegevensverwerking de privacyrisico's in kaart worden gebracht. Op basis van een DPIA kunnen maatregelen worden getroffen om de risico's te minimaliseren of uit te sluiten. In artikel 4c van de Wpg is een verplichting opgenomen voor het uitvoeren van een DPIA op het moment een verwerking waarschijnlijk een hoog risico voor de rechten en vrijheden van personen oplevert.

Voor Vechtstromen geldt als uitgangspunt dat bij iedere nieuwe verwerking van politiegegevens, evenals bij wijzigingen in bestaande verwerkingen, een DPIA wordt uitgevoerd. Daarnaast wordt deze DPIA ten minste eenmaal per drie jaar herzien. Zo is er een DPIA gedaan op de Wpg-verwerkingen en worden de mitigerende maatregelen planmatig opgepakt. Een DPIA is verplicht omdat politiegegevens

gevoelige gegevens zijn en er sprake is van een ongelijke machtsverhouding tussen de boa en de verdachte. Vechtstromen heeft een Procedure 'Privacy quickscan dpia' opgesteld waarin het proces voor het uitvoeren van een DPIA is opgenomen. In deze procedure wordt onder meer besproken welke partijen betrokken moeten worden en aan welke verplichtingen een DPIA moet voldoen.

11. Audits

In het kader van de Wpg dient eens per 4 jaar een externe audit worden uitgevoerd en moet elk jaar een interne audit worden gehouden (art. 33 Wpg). Deze interne audit vindt plaats als voorbereiding op de externe audit.

Indien uit de resultaten van de externe audit blijkt dat de verwerking van de politiegegevens op onderdelen niet voldoet aan de wettelijke normen, dient Vechtstromen binnen een jaar zorg te dragen voor deze tekortkomingen, met als doel dat deze worden verholpen. Dit vindt plaats a.d.h.v. een 'verbeterplan'. Daarnaast voert Vechtstromen binnen één jaar een hercontrole uit, binnen de onderdelen waarvan het resultaat onvoldoende bleek te zijn.

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.

De FG van de Wpg voor Vechtstromen zendt een afschrift van de controleresultaten van de externe audit en de controleresultaten van de heraudit aan de Autoriteit Persoonsgegevens.

12. Review beleid

Tenzij er tussentijdse relevante ontwikkelingen zijn die om eerdere actualisatie vragen, word het Wpg beleid in elk geval 3-jaarlijks herijkt en de Privacyverklaring Wpg kent een jaarlijkse evaluatie.

13. Vaststelling

Beleid vastgesteld in de bestuursvergadering van d.d. 23 juni 2026

dagelijks bestuur, Waterschap Vechtstromen

de secretaris-directeur,

Aldus vastgesteld in de vergadering d.d. 23 juni.

Het dagelijks bestuur van waterschap Vechtstromen,

dr. S.M.M. Kuks, watergraaf

drs. R.I. Andringa, secretaris

Bijlage 1 Begrippenlijst

De volgende begrippen zijn relevant voor de AVG, Wpg en voorliggend Wpg beleid.

- **AP**
De Autoriteit persoonsgegevens is de Nederlandse gegevensbeschermingsautoriteit en het zelfstandig bestuursorgaan dat in Nederland bij wet als toezichthouder voor de AVG is aangesteld voor het toezicht op het verwerken van politiegegevens.
- **AVG en UAVG**
De Algemene Verordening Gegevensbescherming en de Uitvoeringswet Algemene Verordening Gegevensbescherming.
- **Betrokkene**
Natuurlijk persoon op wie de politiegegevens betrekking hebben. Bij Vechtstromen gaat het om de volgende betrokkenen: inwoners, agrariërs, ondernemers, medewerkers en andere betrokkenen die met ons waterschap te maken hebben.
- **Besluit politiegegevens (Bpg)**
Naast de Wet politiegegevens is er ook een Besluit politiegegevens. Daarin is onder andere vastgelegd aan welke partners de politie in welke gevallen politiegegevens mag verstrekken. Tevens staan daar verbijzonderingen in uit de wet, zoals bijvoorbeeld wie waarvoor geautoriseerd mag worden.
- **Besluit politiegegevens buitengewoon opsporingsambtenaren (Bpg boa)**
In het Bpg boa zijn de bepalingen uit de Wpg en het Besluit politiegegevens (Bpg) uitgewerkt die van overeenkomstige toepassing zijn verklaard op de gegevensverwerkingen van boa's in het kader van opsporingstaken.
- **Datalek**
Bij een datalek gaat het om toegang tot of het vrijkomen van politiegegevens zonder dat dit mag of zonder dat dit de bedoeling is van de betreffen onze organisatie. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van politiegegevens valt onder de definitie van een datalek.
- **Gegevenseffectbeschermingsbeoordeling (geb)**
Indien er sprake is van een verhoogd Privacy risico wordt een zogenaamde gegevensbeschermingseffectbeoordeling (ook wel data protection impact assessment – DPIA genoemd) uitgevoerd om te beoordelen welke beheersmaatregelen er moeten worden getroffen om de Privacy risico's te verkleinen.
- **Persoonsgegevens**
De AVG geeft aan dat een persoonsgegeven alle informatie is over een geïdentificeerde of identificeerbare natuurlijke persoon. Als identificeerbaar wordt beschouwd: een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, bijvoorbeeld op basis van een naam, adresgegevens een identificatienummer, foto's of op basis van een of meer elementen die naar een natuurlijk persoon herleidbaar zijn, zoals de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
- **Politiegegevens**
Politiegegevens zijn politiegegevens die in het kader van de politietaak worden verwerkt.
- **Functionaris Gegevensbescherming (FG)**
De Functionaris Gegevensbescherming heeft een, wettelijk bepaalde (op basis van de AVG), onafhankelijke functie. De FG ziet als onafhankelijke functionaris toe op toepassing en naleving van de AVG en Wpg in onze organisatie.
- **Verantwoordingsplicht**
De essentie van de verantwoordingsplicht is dat de verwerkingsverantwoordelijke (het dagelijks bestuur) kan aantonen dat het verwerken van politiegegevens binnen onze organisatie aan de regels van de AVG voldoet.
- **Wet politiegegevens**
De Wet politiegegevens (Wpg) is een Nederlandse wet die de rechten en de plichten van de politie zelf, maar ook die van de burger regelt, voor wat betreft het verwerken van politiegegevens. Naast de politie moeten ook andere organisaties zich aan de Wpg houden: de bijzondere opsporingsdiensten (BOD) en de buitengewoon opsporingsambtenaren (boa's).
- **Verwerkersovereenkomst**
Wanneer Waterschap Vechtstromen de verwerking van politiegegevens uitbesteedt aan een externe partij, dan is het verplicht om afspraken te maken over de wijze van verwerking van de politiegegevens. Deze afspraken moeten schriftelijk worden vastgelegd.
- **Verwerking**
Iedere handeling met politiegegevens. Dus onder andere registreren, vastleggen, filmen, opnemen, raadplegen, vergelijken, wijzigen, tonen, verstrekken en wissen van politiegegevens.
- **Verwerker**

Een verwerker is een entiteit (natuurlijke persoon, rechtspersoon, instantie of -bestuurs- orgaan) die een verwerking uitvoert binnen het doel en middelen die de verwerkingsverantwoordelijke heeft vastgesteld.

- *Verwerkingsregister*

Het waterschap moet conform de Wpg een register bijhouden van alle gegevensverwerkingen die door of namens het waterschap plaatsvinden. In dit register dient o.a. opgenomen te worden: het doel van de gegevensverwerking, de wettelijke reden (grondslag) van de verwerking, de categorieën van betrokkenen, de soort politiegegevens en met wie deze gegevens gedeeld worden.

- *Verwerkingsverantwoordelijke*

De verwerkingsverantwoordelijke is de entiteit (organisatie) die het doel van en de middelen voor de verwerking van politiegegevens vaststelt. De verwerkingsverantwoordelijke dient te zorgen voor passende waarborgen voor het naleven van de Wpg.

- *Wpg beleid*

Het Wpg beleid geeft Vechtstromen op organisatorisch- en strategisch niveau duidelijkheid over de keuze van de inrichting van eisen uit de Wpg en houvast in het zorgvuldig omgaan met politiegegevens.