

Wpg-beleid

Brabantse Waterschappen 2025 – 2027

Voor alles wat je doet met politiegegevens

Eigenaar:

A. Meuleman (Secretaris-Directeur Waterschap Brabantse Delta)
P. Verlaan (Secretaris-Directeur Waterschap Aa en Maas)
H. Kielenstein (Secretaris-Directeur Waterschap De Dommel)

Gemandateerd eigenaar:

Procesmanager VTH, Waterschap Brabantse Delta
Afdelingshoofd VTH, Waterschap Aa en Maas

Contactpersoon:

Manager Toezicht & Handhaving, Waterschap De Dommel

Opgesteld door:

... (Waterschap Aa en Maas)
... (Waterschap Aa en Maas)

Quality Assurance:, FG

Versie 0.5 Te reviewen in 2027 of zoveel eerder als noodzakelijk is.

Versiebeheer

Versie	Status	Auteur(s)	Toelichting
0.1	Concept	...	Initieel Document
0.2	Concept	...	Review ... verwerkt
0.3	Concept	...	Review ... (Waterschap Aa en Maas) verwerkt
0.4	Concept	...	Review ... (Waterschap De Dommel), ... (Waterschap Brabantse Delta) verwerkt
0.5	Concept	...	Review ... (Waterschap De Dommel), ... (Waterschap Brabantse Delta), ... QA door ... FG

Inhoud

1	Inleiding	1
1.1	Over dit document	1
1.2	Relatie met de applicatie BRS	1
1.3	Wpg en AVG	1
1.4	Missie van het waterschap m.b.t. het beschermen van politiegegevens	1
1.5	Het waterschap en het verwerken van Politiegegevens.....	1
2	Kaders	2
2.1	Scope.....	2
2.2	Bereik.....	2
2.3	Werking en evaluatie	3
2.4	Verantwoordelijkheid verwerking politiegegevens.....	3
2.5	Rollen.....	3
2.6	Wet- en regelgeving.....	4
2.7	Landelijke en Europese ontwikkelingen	4
Beleid		5
2.8	Doelstellingen Wpg-beleid	5
2.9	Sturing.....	5
2.10	Risicomanagement	5
2.11	Uitgangspunten voor privacy	5
2.11.1	Rubricering van politiegegevens.....	5
2.11.2	Het waterschap gaat passend en veilig om met politiegegevens	6
2.11.3	Verantwoordelijkheid voor het juist verwerken van persoonsgegevens	6
2.11.4	Kennisuitwisseling en opbouw	7
2.11.5	Samenwerking met marktpartijen en partners	7
2.11.6	Verwerkersovereenkomst	7
2.11.7	Register van verwerkingen	7
2.11.8	Privacy by design and by default	8
2.11.9	Centralisatie datavoorziening.....	9
2.11.10	Privacy risico's in kaart brengen	9
2.12	Rechten van betrokkenen.....	9
2.13	Logging	10
2.14	Datalek.....	11
2.15	Documentatieplicht	11
2.16	Noodzakelijkheid, rechtmatigheid, vermelding herkomst en doelbinding.....	11
2.17	Proportionaliteit, noodzakelijkheid en subsidiariteit	12
2.18	Juistheid en volledigheid politiegegevens	12
2.19	Onderscheid feiten en persoonlijk oordeel	12
2.20	Boetes.....	12
3	Organisatie van beschermen van politiegegevens	12
4	Controle, naleving	14

4.1	Controles.....	14
4.2	Audits	15
5	Bijlagen.....	17
5.1	Bijlage 1 – Afkortingen	17
5.2	Bijlage 2 – Belangrijke definities	17
5.3	Bijlage 3 – Wettelijke grondslagen voor het verwerken van persoonsgegevens	18
5.4	Bijlage 4 – Bewaartermijnen Wpg	20
5.5	Bijlage 5 – Geraadpleegde bronnen	20

1 Inleiding

1.1 Over dit document

De Wet politiegegevens (Wpg) is een Nederlandse wet die de rechten en plichten regelt voor organisaties die politiegegevens verwerken, waaronder waterschappen die werken met Buitengewoon Opsporingsambtenaren (BOA's). Politiegegevens zijn persoonsgegevens die worden verwerkt in het kader van opsporing en handhaving.

Dit document is in het bijzonder bestemd voor zowel de Buitengewoon Opsporingsambtenaren (BOA's), als voor de bevoegd functionaris, FG, CISO, administratief personeel, beleidsmedewerkers, leidinggevenden, (privacy)adviseurs en auditors die in aanraking komen met politiegegevens.

1.2 Relatie met de applicatie BRS

De Brabantse Waterschappen hebben ervoor gekozen om de Wpg voor een belangrijk deel te implementeren in de applicatie BRS (BOA Registratie Systeem). Dit document kan niet los van die implementatie worden gezien. Een deel van de taken en verplichtingen die de Wpg aan de Brabantse Waterschappen oplegt is in deze applicatie geïmplementeerd en geborgd. Waar dit van toepassing is zal dit document dan ook naar BRS verwijzen.

1.3 Wpg en AVG

Waterschappen die werken met BOA's, moeten zorgen voor een duidelijk beleid en procedures die voldoen aan zowel de Algemene Verordening Gegevensbescherming (AVG) als de Wpg.

De AVG is niet van toepassing op gegevens die worden verwerkt voor de opsporing of vervolging van strafbare feiten. Voor dat soort gegevens geldt de Wpg. Dit Wpg-beleid document staat daarom naast het Privacy beleid Brabantse Waterschappen.

1.4 Missie van het waterschap m.b.t. het beschermen van politiegegevens

Het waterschap wil een betrouwbare overheid zijn voor de burgers, een betrouwbare partner voor andere overheden, bedrijven en organisaties en een betrouwbare werkgever voor zijn medewerkers. Het waterschap wil daarom de politiegegevens die door het waterschap worden verwerkt optimaal beschermen. Het waterschap draagt zorg voor:

- Voldoende technische en organisatorische beveiliging van politie- en persoonsgegevens (o.m. op basis van de Baseline Informatiebeveiliging Overheid, kortweg BIO);
- Bewustwording bij het bestuur, management en de medewerkers over de juiste verwerking van politie en persoonsgegevens (door middel van onder andere Wpg trainingen, berichten op Spraakwater, richtlijnen/protocollen);
- Het kunnen uitoefenen door betrokkene van zijn rechten (beschreven in de privacyverklaring Wpg op de websites van de drie Brabantse waterschappen).

1.5 Het waterschap en het verwerken van Politiegegevens

Persoonsgegevens

Persoonsgegevens zijn gegevens betreffende een identificeerbaar of geïdentificeerde natuurlijke persoon. Het gaat dus om alles dat in verband kan worden gebracht met een natuurlijke persoon: naam, foto, telefoonnummer, personeelsnummer, maar ook een bankrekeningnummer, gps-positie of kenteken. Audio- en video-opnames zijn ook persoonsgegevens.

Belangrijk is dat de persoon nog niet geïdentificeerd hoeft te zijn. Het is al een persoonsgegeven als het tot identificatie kán leiden.

Bijzondere persoonsgegevens

Binnen de AVG en Wpg worden bijzondere categorieën persoonsgegevens omschreven als gevoelige gegevens die extra bescherming vereisen vanwege hun aard. De bijzondere categorieën persoonsgegevens omvatten onder andere:

1. Biometrische identificatiegegevens
2. Gezondheidsgegevens
3. Juridische gegevens, strafrechtelijke veroordelingen en/of opgelegde verboden
4. Beeld-, audio- of video-opnamen (voor bijzondere persoonsgegevens)
5. Filosofische of religieuze overtuigingen
6. Politieke overtuigingen
7. Raciale en etnische gegevens
8. Seksuele gegevens
9. Vakbondslidmaatschap

Deze categorieën persoonsgegevens worden als bijzonder beschouwd omdat ze informatie bevatten die zeer persoonlijk is en waarvan de verwerking grote gevolgen kan hebben voor de betrokkenen. Daarom vereist de Wpg dat dergelijke gegevens alleen mogen worden verwerkt als het strikt noodzakelijk is voor de uitvoering van de wettelijke taken van de politie en dat er passende beveiligingsmaatregelen worden getroffen om deze gegevens te beschermen.

Politiegegevens

Een politiegegeven is een persoonsgegeven of een bijzonder persoonsgegeven dat verwerkt wordt in het kader van de opsporingstaak. Hiervoor geldt de Wpg. Een politiegegeven is dus een specifieke versie van een persoonsgegeven.

2 Kaders

2.1 Scope

Dit Wpg-beleid is van toepassing op de verwerking van politie gegevens die zich bevinden binnen de informatiehuishouding van het gehele waterschap en op de informatie-uitwisseling van het waterschap met andere organisaties.

Binnen de scope van dit beleid vallen ook de diensten die door externe partijen worden uitgevoerd namens het waterschap. Voor deze diensten en dienstverlening geldt dat desbetreffende partijen zich aansluiten bij het beleid van het waterschap en de hieruit voortkomende beveiligingsmaatregelen.

2.2 Bereik

Locaties waterschap:

De Wpg en daarmee ook dit beleid is van toepassing:

- op alle locaties van het waterschap: hoofdkantoor, districts- of regiokantoren, gemalen, rioolwaterzuiveringsinstallaties en objecten in beheer van het waterschap;
- op iedere locatie waar medewerkers zich met persoonsgegevens van het waterschap bevinden (veldwerk, thuiswerken) al dan niet ondersteund met mobiele apparatuur¹.

Waar bevinden zich de politiegegevens?

De Wpg en daarmee ook dit beleid geldt voor politiegegevens:

- die geautomatiseerd worden verwerkt;
- die in een bestand zijn opgenomen;
- die bedoeld zijn om in een bestand te worden opgenomen;
- die op papier worden verwerkt.

Ook kunnen politiegegevens van het waterschap door derden verwerkt worden, waarbij het waterschap verwerkingsverantwoordelijke blijft.

¹ In toenemende mate wordt (vertrouwelijke) informatie, waaronder politie en persoonsgegevens, ontsloten op mobiele apparaten die geen onderdeel zijn van de traditionele IT-voorzieningen (laptops, smartphones, tablets, telewerkplek etc.) en zich veelal buiten de beschermde fysieke omgeving (kantoren) van het waterschap bevinden. Bij het toepassen van deze technologie gelden onverminderd de vereisten van de Wpg en dezelfde beveiligingsuitgangspunten als voor de traditionele voorzieningen. Het belangrijke verschil is de bewustwording van de individuele bestuurder en/of medewerker van de eigen verantwoordelijkheid bij het omgaan met politiegegevens en informatie via hun mobiele apparaten.

Het Wpg-beleid geldt voor:

- bestuurders;
- alle medewerkers van het waterschap, inclusief tijdelijk personeel, ingehuurd personeel en stagiairs.

2.3 Werking en evaluatie

Om te voldoen aan de Wpg-wetgeving moeten alle organisaties waar BOA's actief zijn eens in de vier jaar een externe audit laten uitvoeren. De resultaten van deze audit moeten, conform een vast rapportageformat, aan de Autoriteit Persoonsgegevens worden opgeleverd.

Naast de verplichte externe audit, wordt de werking van dit Wpg-beleid door middel van een interne audit management-cyclus (PDCA) ieder jaar getoetst op juiste werking en aan de geldende normen. Indien het noodzakelijk is (zoals bijvoorbeeld bij wijziging van de toepasselijke regelgeving) wordt het Wpg-beleid tussentijds aangepast. Over de wijzigingen wordt vervolgens gecommuniceerd naar belanghebbenden.

De audits zijn verder toegelicht in paragraaf 4.2 Audits.

2.4 Verantwoordelijkheid verwerking politiegegevens

Het verwerken van politiegegevens vindt plaats in opsporing- en vervolgingsprocessen die binnen afdelingen zijn belegd. Dit betekent dat management van deze afdelingen binnen het waterschap de primaire verantwoordelijkheid dragen voor een goede verwerking en beveiliging van persoonsgegevens op hun afdeling en in hun processen.

Bekendheid met dit Wpg-beleid is daarvoor de minimum vereiste.

2.5 Rollen

Specifiek voor de bescherming van politiegegevens zijn de volgende rollen geïntroduceerd:

Rol	Relevantie voor Wpg-beleid
Functionaris gegevensbescherming (FG)	• Onafhankelijk informeren en adviseren van het bestuur van het waterschap, het management en de medewerkers over hun verplichtingen op grond van de AVG en Wpg; • Binnen het waterschap toezien op de naleving van de AVG en Wpg; • Gevraagd en ongevraagd advies geven met betrekking tot een Data Protection Impact Assessment (DPIA); • Neemt deel aan de Privacydesk; • Werkt samen met en is contactpersoon voor de Autoriteit Persoonsgegevens (AP); • Aanspreekpunt voor vragen en klachten over de uitvoering van het beleid.
Bevoegd functionaris (BF)	• Heeft voldoende kennis en vaardigheden m.b.t. Wpg; • Draagt zorg voor artikel 9 verwerking door middel van doel omschrijven en vastleggen (zie Wpg artikel #32, via BRS); • Verleent autorisatie van personen voor betreffende verwerking (via BRS); • Bepaalt of gegevens voor andere doeleinden mogen worden gebruikt (zie Wpg artikel #9, lid3, via BRS); • Zorgt ervoor dat voor alle gegevens de herkomst en wijze van verkrijgen wordt vastgelegd (zie Wpg artikel #3, lid5, via BRS); • Bewaakt dat gegevens rechtmatig worden verkregen en verwerkt, waarbij met name wordt gelet op de termijnen (via BRS); • Werkt nauw samen met FG/CISO, privacy jurist en managers.

BOA	• Is verantwoordelijk voor het naleven van de werkafspraken en instructies met betrekking tot de Wpg; • Zorgt voor correcte en veilige verwerking van politiegegevens.
------------	---

2.6 Wet- en regelgeving

Het Wpg-beleid Brabantse Waterschappen is afgeleid van de wet- en regelgeving die op het waterschap van toepassing is. Voor privacy en Wpg is de meest relevante regelgeving:

- Algemene Verordening Gegevensbescherming (AVG);
- Uitvoeringswet Algemene verordening gegevensbescherming (UAVG).
- Wet politiegegevens (Wpg)
- Algemene Wet Bestuursrecht (Awb)
- Besluit Politiegegevens buitengewoon opsporingsambtenaren

2.7 Landelijke en Europese ontwikkelingen

Landelijke ontwikkelingen

1) Aanpassing in Nationale Regelgeving:

De Wet politiegegevens (Wpg) wordt regelmatig aangepast om te voldoen aan nieuwe inzichten en ontwikkelingen op het gebied van gegevensbescherming en privacy. Recente wijzigingen hebben betrekking op de versterking van de beveiliging van politiegegevens en de implementatie van strengere controlemechanismen. Dit is noodzakelijk om te voldoen aan de steeds strengere eisen op het gebied van privacy en gegevensbescherming.

2) Toezicht en Handhaving:

De AP heeft haar rol als toezichthouder uitgebreid en legt meer nadruk op handhaving van de Wpg. Dit betekent dat er strengere controles en audits plaatsvinden om te garanderen dat organisaties die politiegegevens verwerken, zoals gemeenten en waterschappen, voldoen aan de wettelijke eisen.

Europese ontwikkelingen

1) Cyber Resilience Act:

De EU werkt aan de "Cyber Resilience Act", die gedetailleerde cyber security-eisen stelt voor producten met digitale elementen, waaronder hardware en software. Dit heeft implicaties voor de verwerking van politiegegevens, aangezien producten die dergelijke gegevens verwerken moeten voldoen aan strenge beveiligingseisen om te voorkomen dat gevoelige gegevens in verkeerde handen vallen.

2) Versterking van de Algemene Verordening Gegevensbescherming (AVG):

De AVG blijft een belangrijke invloed uitoefenen op de Wpg. De EU is voortdurend bezig met het aanscherpen van de regelgeving rondom gegevensbescherming en privacy. Dit zorgt ervoor dat de Wpg in lijn blijft met Europese standaarden en dat er consistentie is in de bescherming van persoonsgegevens binnen de EU.

Conclusie

De ontwikkelingen op zowel nationaal als Europees niveau tonen een duidelijke trend naar strengere regelgeving en betere bescherming van gevoelige gegevens waaronder politiegegevens. Organisaties zoals waterschappen moeten proactief blijven om te voldoen aan deze veranderende eisen, waarbij aandacht voor beveiliging, transparantie en naleving van de wet cruciaal is. Het bijhouden van deze ontwikkelingen en het implementeren van de vereiste maatregelen zal helpen om de privacy van betrokkenen te waarborgen en boetes en andere sancties te voorkomen.

Beleid

2.8 Doelstellingen Wpg-beleid

Het waterschap is een moderne functionele overheid met oog voor wat de samenleving van ons vraagt, waarbij het waarborgen van privacy en naleven van Wpg-wetgeving voorwaarden zijn. Dit Wpg-beleid geeft hiervoor principes die belangrijk zijn voor het afwegen van belangen. Bij de borging van de Wpg binnen het waterschap, wordt bij het uitvoeren van deze taken rekening gehouden met de volgende uitgangspunten:

- *Recht op Privacy:* Ieder individu heeft recht op privacy en bescherming van zijn of haar politiegegevens om nadelige gevolgen in de persoonlijke sfeer te voorkomen of te beperken.
- *Voldoen aan Wpg-bepalingen:* Het waterschap voldoet aan de wettelijke bepalingen uit de Wpg, zoals de aantoonbaarheid van het voldoen aan de Wpg en het uitvoeren van de rechten van betrokkenen.
- *Risicogerichte Aanpak:* Er wordt continu een afweging gemaakt tussen de verwerking en het risico dat de verwerking (mogelijk voor de betrokkene) met zich meebrengt.
- *Privacy by Design en by Default:* Het waterschap past "privacy by design en by default" toe bij het ontwikkelen van nieuwe informatiesystemen, waardoor er al in de beginfase rekening wordt gehouden met de bescherming van politiegegevens. De aandacht voor privacy blijft gedurende de gehele levensduur van het systeem bestaan om de beveiliging van politiegegevens te optimaliseren.

Door deze uitgangspunten te volgen, zorgt het waterschap ervoor dat de verwerking van politiegegevens in lijn is met de Wpg en dat de privacy van betrokkenen gedurende de gehele levenscyclus van de gegevensverwerking wordt gewaarborgd.

2.9 Sturing

Het proces "verwerken en beschermen politiegegevens" is een cyclisch proces (PDCA) en wordt opgenomen in de bestaande planning & control cyclus van de organisatie. Dit houdt in dat de activiteiten die in het kader van de Wpg moeten worden uitgevoerd in een meer jaarlijkse planning zijn opgenomen.

2.10 Risicomanagement

Beschermen en verwerken politiegegevens is gebaseerd op risicomanagement. Omdat er beperkingen zijn in menskracht, geld en middelen wordt vastgesteld waar de inzet ervan het meeste effect heeft op het bijdragen aan de organisatiedoelstellingen en het voorkomen van schade voor betrokkenen en aan de organisatie.

2.11 Uitgangspunten voor privacy

De uitgangspunten voor politiegegevens zijn in de volgende 11 paragrafen verwoord.

2.11.1 Rubricering van politiegegevens

De AVG onderkent de volgende persoonsgegevens:

- (Gewone) persoonsgegevens;
- Bijzondere persoonsgegevens;
- Strafrechtelijke persoonsgegevens;
- Nationaal identificatienummer (Burgerservicenummer, BSN).

Strafrechtelijke gegevens onder de AVG zijn geen bijzondere persoonsgegevens. Het is een aparte categorie en de verwerking van strafrechtelijke gegevens is verboden. Tenzij een beroep gedaan kan worden op een specifieke wettelijke uitzondering (zoals de Wpg) én op één van de grondslagen voor het verwerken van gewone persoonsgegevens (zie hiervoor Bijlage 3 – Wettelijke grondslagen voor het verwerken van persoonsgegevens).

Voor het waterschap is het van belang dat strafrechtelijke gegevens alleen verwerkt mogen worden onder de Wpg.

Of een persoonsgegeven een persoonsgegeven onder de AVG is of een politiegegeven onder de Wpg hangt af van de aard van de verwerking van het persoonsgegeven. In onderstaande tabel is dit weergegeven.

Persoonsgegevens	Verwerking voor:	Onderhavig aan wetgeving:	Soort gegeven:
(gewoon) persoonsgegevens	Toezicht	AVG	Persoonsgegevens
	Opsporing en vervolging	Wpg	Politiegegevens
Bijzonder persoonsgegevens	Toezicht	AVG	Persoonsgegevens
	Opsporing en vervolging	Wpg	Politiegegevens
Strafrechtelijk persoonsgegevens	Opsporing en vervolging	Wpg	Politiegegevens

2.11.2 Het waterschap gaat passend en veilig om met politiegegevens

- Hierbij maakt het waterschap gebruik van gangbare beveiligingsnormen en risicomethodieken (zoals o.a. opgenomen in de BIO);
- controle en audits zijn een onderdeel van het bestaande kwaliteitssysteem binnen het waterschap;
- het waterschap beveiligt met gezond verstand: €100 euro uitgeven om een waarde van €1 te beschermen is geen optie).

2.11.3 Verantwoordelijkheid voor het juist verwerken van persoonsgegevens

Verwerken van politiegegevens is een managementverantwoordelijkheid. Dit betekent dat leidinggevenden/procesmanagers de primaire verantwoordelijkheid dragen voor een goede informatiebeveiliging op hun afdeling/binnen hun proces.

BOA's gebruiken het systeem dat is aangewezen voor verwerking van Wpg gegevens² conform de wettelijke bepalingen en de gebruikershandleiding(en) en voorkomen dat er zonder noodzaak registraties van politiegegevens buiten BRS worden aangelegd ('schaduwsystemen').

BOA's laten alle gegevensinvoer achterwege die niet absoluut noodzakelijk is op grond van de in de wet genoemde doeleinden.

Rechtstreekse verstrekking vindt alleen plaats op basis van de Wet op de justitiële documentatie en op de verklaringen omtrent het gedrag BES.

Politiegegevens worden alleen verstrekt aan anderen dan politie en Koninklijke marechaussee voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wet politiegegevens en het Besluit politiegegevens zijn genoemd.

Nota bene: Het waterschap verstrekt geen politiegegevens aan anderen dan politie en Koninklijke marechaussee. Indien dit toch noodzakelijk blijkt, dan verloopt de verstrekking via de BF en draagt de BF er zorg voor dat deze verwerking in het verwerkingsregister wordt opgenomen.

Nota bene: Het verstrekken van politiegegevens aan bevoegde autoriteiten in andere lidstaten van de EU of aan organen en instanties zoals bedoeld in art. 15a voor zover dat voortvloeit uit een rechtsinstrument op grond van het verdrag betreffende de werking van de EU, vindt niet plaats.

² BRS

2.11.4 Kennisuitwisseling en opbouw

Tussen de Brabantse waterschappen vindt kennisuitwisseling plaats over informatieveiligheid, privacy en de Wpg.

De Brabantse waterschappen participeren in programma's en overlegorganen binnen en buiten de sector ten aanzien van informatiebeveiliging en privacy. Voorbeelden hiervan zijn:

- het programma Informatiebeveiliging en Privacy van het Waterschapshuis (HWH Amersfoort). Het waterschap neemt deel aan de CPW (Coördinatoren privacy waterschappen);
- Het CIP, een publiek-private netwerkorganisatie met als doel faciliteren van kennisdeling op het gebied van informatiebeveiliging en privacy.

Samen met andere sectoren en het Nationaal Cyber Security Center (NCSC) wordt kennis uitgewisseld.

Er is nauwe samenwerking met het CERT-WM³ over bedreigingen en weerbaarheid tegen actuele dreigingen.

2.11.5 Samenwerking met marktpartijen en partners

Waar privacy-expertise nodig is die binnen het waterschap ontbreekt, wordt gebruik gemaakt van de kennis van marktpartijen en partners. Dit doen we ook als we een onafhankelijke externe blik nodig hebben, bijvoorbeeld voor testen en audits.

2.11.6 Verwerkersovereenkomst

Het waterschap kan werkzaamheden uitbesteden aan derden. Daarvoor is het soms nodig dat het waterschap persoonsgegevens verstrekt aan deze andere partij. Wanneer die partij politiegegevens verwerkt namens het waterschap is de andere partij "verwerker" in de zin van de Wpg. Het waterschap is en blijft verwerkingsverantwoordelijke met betrekking tot deze persoonsgegevens. Voor de Brabantse waterschappen verwerkt NatuurNetwerk BV politiegegevens in de applicatie BRS. NatuurNetwerk BV is hiermee verwerker. Het waterschap is de verwerkingsverantwoordelijke.

Kenmerkend van een verwerker is:

- dat deze niet aan het gezag van het waterschap is onderworpen;
- dat deze niet zelf doel en middelen van de verwerking van de persoonsgegevens bepaalt.

Dit is en blijft de verantwoordelijkheid van het waterschap.

De Wpg bepaalt dat met iedere verwerker vóór de verwerking van politiegegevens afspraken worden gemaakt en vastgelegd over het verwerken en beveiligen van de deze gegevens. Deze overeenkomst wordt de "verwerkersovereenkomst" genoemd.

- Informatie over het al dan niet afsluiten van een verwerkersovereenkomst bij een overeenkomst met een verwerker is in te winnen bij de Privacydesk;
- het waterschap gebruikt de door het CPW opgestelde modellenverwerkersovereenkomsten;
- het waterschap houdt in het verwerkingsregister een overzicht bij van alle door het waterschap afgesloten verwerkersovereenkomsten.

2.11.7 Register van verwerkingen

De Wpg verplicht het waterschap om een register bij te houden van alle verwerkingen van politiegegevens. Conform Wpg artikel 31d lid 1 legt het waterschap de volgende informatie vast:

- De naam en contactgegevens van de verwerkingsverantwoordelijke
- De naam en contactgegevens van de FG
- 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;

³ Computer Emergency Response Team Water Management

- 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 politie gegevens 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;
- Of er een verwerkersovereenkomst met een verwerker is afgesloten.

Voor het up-to-date houden van het register van verwerkingen zijn (proces)managers verantwoordelijk voor:

- Het tijdig aanleveren van de juiste gegevens;
- Het periodiek actueel houden van het register en het registreren van nieuwe en bestaande verwerkingen binnen het Wpg-domein;
- Het uitvoeren van een zichtbare periodieke actualisatie van het verwerkingsregister conform de procedure.

Nota bene: Het waterschap neemt geen besluiten die uitsluitend gebaseerd zijn op geautomatiseerde verwerking (profilering).

Nota bene: Geautomatiseerde vergelijking met andere politiegegevens of met andere dan politiegegevens vindt niet plaats. Indien dit toch noodzakelijk is, dan kan dit alleen via de BF plaatsvinden en zorgt de BF ervoor dat deze verwerking in het verwerkingsregister wordt opgenomen.

Nota bene: Het waterschap geeft geen politiegegevens door aan derde landen. Indien dit toch noodzakelijk is, dan kan dit alleen via de BF plaatsvinden en zorgt de BF ervoor dat deze verwerking in het verwerkingsregister wordt opgenomen.

Nota bene: Het waterschap verstrekt geen politiegegevens structureel aan derden voor samenwerkingsverbanden. Indien dit toch noodzakelijk is, dan kan dit alleen via de BF plaatsvinden en zorgt de BF ervoor dat deze verwerking in het verwerkingsregister wordt opgenomen.

2.11.8 Privacy by design and by default

Privacy by design and by default heet in de Wpg ‘gegevensbescherming door beveiliging en ontwerp (art. 4a en 4b van de Wpg)’.

Bij het waterschap wordt vanaf het begin van de ontwikkeling van een proces, systeem of dienst rekening gehouden met privacy (het “privacy by design” en “privacy by default” principe). Dit houdt in dat er zeer kritisch gekeken wordt naar onder andere dataminimalisatie en het gebruik van andere technieken om persoonsgegevens in (informatie)systemen te beschermen. Daarbij zijn de volgende uitgangspunten van toepassing:

Uitgangspunt	Beschrijving
Proactief en preventief	Privacy is vanaf de initiatie een aandachtspunt. Begin met privacy in een zo vroeg mogelijk stadium, dus bij de beleidsvorming en de eerste opzet van de proces/systeemarchitectuur en win advies in bij de Privacydesk.
Privacy by default	Als de betrokkene in een systeem een keuze kan maken uit meerdere opties, dan is de meest strikte bescherming van privacy de standard optie. De betrokkene hoeft zelf niets te doen om de privacy optimaal te beschermen.
Privacy geïntegreerd in het ontwerp	Privacy maatregelen zijn integraal onderdeel van de informatieverwerking. Dit geldt voor de technische systemen én de processen die de informatie verwerken.
Privacy by design	Privacy by design waarborgt de privacy, inclusief de beveiliging, gedurende de gehele levenscyclus van de persoonsgegevens van verzamelen/ontwerpen tot vernietiging. Het zorgdragen voor veiligheid is geen eenmalige actie.
Zichtbaarheid en transparantie – houd het open	Inzicht en transparantie over hoe persoonsgegevens worden verwerkt moet mogelijk zijn voor zowel de betrokkene, de eigen organisatie en de toezichthouder. Op de website van het waterschap is voor iedereen de privacyverklaring van het waterschap te lezen.

2.11.9 Centralisatie datavoorziening

Het beleid van het waterschap is om politiegegevens centraal op te slaan. Daarvoor wordt gebruik gemaakt van BRS. Zo ontstaat een centrale plek waar alle gegevens opgeslagen kunnen worden en is er maximale controle op de toegang en behandeling van deze gegevens. Het helpt ook om te voldoen aan eisen uit de Wpg (zoals juistheid, opslagbeperking, minimale gegevensverwerking en uitoefening van rechten van betrokkenen).

Er is een procedure ingericht om toegang te verlenen tot de politiegegevens in BRS. Hiervoor is een autorisatiematrix opgesteld waarin, op basis van functie of rol, medewerkers worden geautoriseerd binnen BRS. De autorisaties worden minimaal tweemaal per jaar gecontroleerd en de resultaten van de controle worden vastgelegd.

2.11.10 Privacy risico's in kaart brengen

Een DPIA is een methode om in een vroeg ontwikkelstadium op een gestructureerde manier risico's met betrekking tot privacy- en politiegegevens in beeld te brengen alvorens een nieuw(e) werkproces/applicatie/software wordt aangeschaft of in gebruik genomen.

Een DPIA is op grond van de Wpg verplicht als de (nieuwe/gewijzigde) verwerking waarschijnlijk een hoog privacy risico oplevert voor de betrokkenen. Dat is in ieder geval het geval bij:

Wanneer een soort verwerking van politietgegevens, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context of doelen ervan, waarschijnlijk een hoog risico voor de rechten en vrijheden van personen oplevert, voert de verwerkingsverantwoordelijke voorafgaande aan de verwerking een beoordeling uit van het effect van de voorgenumen verwerkingsactiviteiten op de bescherming van persoonsgegevens.

In principe wordt altijd een advies ingewonnen bij de Privacydesk over het al dan niet uitvoeren van een DPIA.

Een uitgevoerde DPIA kan worden herhaald als er zich wijzigingen in de verwerking of in de "omgeving" (bv jurisprudentie) voordoen.

Een DPIA voor de verwerking van politiegegevens komt grotendeels overeen met de DPIA voor de verwerking van persoonsgegevens. Omdat er toch enkele verschillen zijn, is ervoor gekozen om twee aparte DPIA's templates op te stellen. De Wpg-DPIA is geen onderdeel van dit Wpg-beleid en is apart opgeleverd.

2.12 Rechten van betrokkenen

Betrokkenen hebben op grond van de Wpg diverse rechten. De rechten van betrokkenen onder de Wpg zijn vergelijkbaar met, maar in bepaalde opzichten ook strenger en specifiekere dan die onder de AVG. De verschillen zijn inzichtelijk gemaakt in de onderstaande tabel.

1. Recht op Inzage

Betrokkenen hebben het recht om te weten of hun persoonsgegevens worden verwerkt en, indien dat het geval is, om toegang te krijgen tot die gegevens en bepaalde informatie daarover.

2. Recht op Rectificatie

Betrokkenen kunnen verzoeken om onjuiste persoonsgegevens te corrigeren. Dit recht is van toepassing als de gegevens onjuist of onvolledig zijn.

3. Recht op Verwijdering

Betrokkenen hebben het recht om te verzoeken dat hun persoonsgegevens worden verwijderd als deze onrechtmatig worden verwerkt of niet langer nodig zijn voor de doeleinden waarvoor ze zijn verzameld of verwerkt.

4. Recht op Beperking van de Verwerking

Betrokkenen kunnen de verwerking van hun persoonsgegevens beperken onder bepaalde omstandigheden, zoals wanneer de juistheid van de gegevens wordt betwist.

5. Recht van Bezwaar

Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van hun persoonsgegevens, tenzij de verwerking noodzakelijk is voor de uitvoering van de taak van de verwerkingsverantwoordelijke.

6. Recht op Kennisgeving van Datalekken

Betrokkenen moeten worden geïnformeerd over datalekken die waarschijnlijk een hoog risico inhouden voor hun rechten en vrijheden, tenzij er specifieke redenen zijn om deze kennisgeving uit te stellen of achterwege te laten, bijvoorbeeld in het belang van een strafrechtelijk onderzoek.

Recht van betrokkene	Wpg	Toepassingsomstandigheden Wpg	AVG
Recht op inzage	Ja, met beperking in belang van het onderzoek	Kan worden beperkt als inzage het onderzoek zou kunnen belemmeren of gevaar oplevert voor informanten, getuigen of andere derden.	Ja, algemeen recht zonder specifieke beperkingen
Recht op rectificatie	Ja, bij onjuiste of onvolledige gegevens	Toegestaan tenzij correctie de lopende opsporing of vervolging kan belemmeren..	Ja, algemeen recht
Recht op verwijdering	Ja, met specifieke uitzonderingen	Niet toegestaan als gegevens noodzakelijk zijn voor lopend onderzoek of strafvervolging, of als verwijdering de veiligheid van individuen kan schaden.	Ja, algemeen recht
Recht op beperking	Ja, onder bepaalde omstandigheden	Toegestaan bij betwisting van juistheid, onrechtmatige verwerking, of als gegevens niet langer nodig zijn, maar noodzakelijk voor rechtsvordering.	Ja, algemeen recht
Recht van bezwaar	Ja, tenzij noodzakelijk voor de politietaak	Niet toegestaan als verwerking noodzakelijk is voor de uitvoering van de politietaak, bijvoorbeeld bij lopende onderzoeken of openbare handhaving.	Ja, algemeen recht
Recht op kennisgeving van datalekken	Ja, maar kan worden uitgesteld in belang van onderzoek	Uitstel mogelijk als melding de opsporing of vervolging kan belemmeren of als er veiligheidsrisico's voor individuen of het onderzoek zelf bestaan.	Ja, direct melden zonder uitzonderingen

Het waterschap draagt er zorg voor dat betrokkenen op transparante en eenvoudige wijze hun Wpg rechten kunnen uitoefenen conform de wettelijke voorwaarden en termijnen.

Het waterschap biedt een digitaal formulier aan waarmee via de website van het waterschap op eenvoudige wijze door betrokkene een verzoek kan worden gedaan inzake de verwerking van de Wpg persoonsgegevens.

De betrokkene ontvangt uiterlijk binnen de daarvoor gestelde wettelijke termijn een reactie op zijn verzoek aangaande de verwerking van zijn Wpg persoonsgegevens.

2.13 Logging

De Wpg verplicht tot het langs elektronische weg vastleggen van de volgende verwerkingen van politiegegevens:

Het verzamelen, wijzigen, raadplegen, verstrekken, doorgeven, combineren of vernietigen van politiegegevens.

Deze logging wordt uitsluitend gebruikt voor de controle van de rechtmatigheid van de gegevensverwerking, voor interne controles, ter waarborging van de integriteit en de beveiliging van de politiegegevens en voor strafrechtelijke procedures.

2.14 Datalek

Alle constatering en vermoedens van een inbreuk in verband met politiegegevens worden gemeld en vastgelegd.

Het waterschap heeft een helder en up-to-date datalekprotocol, waarmee effectief en efficiënt gehandeld kan worden bij een geconstateerd (mogelijk) datalek:

- melden van een datalek door een burger kan telefonisch (telefoonnummer op de website) tijdens openingstijden van het kantoor en 24 uur per dag 7 dagen per week via het contactformulier op de website;
- de Helpdesk ICT is de eerste lijn waar een (mogelijk) datalek intern gemeld wordt en volgens het protocol wordt opgepakt;
- het protocol voorziet in het doen van een melding bij de Autoriteit Persoonsgegevens als dat aan de orde is;
- het datalekprotocol geeft aan wanneer opschaling naar een calamiteit aan de orde is.
- hoe te handelen bij een calamiteit betreffende persoonsgegevens is opgenomen in de calamiteitenplannen van het waterschap;
- een evaluatie van het datalek ter lering en verbetering is een verplichte stap in het protocol.
- eventuele melding bij de toezichthoudende autoriteit van een datalek vindt na consultatie met de FG plaats.

In aanvulling op het (AVG) Datalek protocol, geldt voor Wpg datalek protocol het volgende:

- 1) Voor politiegegevens kan de melding aan de AP worden uitgesteld, beperkt of achterwege gelaten als dat de opsporing, vervolging of berechting zou kunnen belemmeren.
- 2) Alle incidenten waarbij de beveiliging van persoonsgegevens is geschonden (zoals datalekken), moeten schriftelijk worden vastgelegd.
Dit omvat de feiten rond de inbreuk, de gevolgen ervan, en de maatregelen die zijn genomen om de inbreuk te corrigeren.

2.15 Documentatieplicht

Het waterschap heeft een documentatieplicht. Hiervoor zijn processen ingericht om het volgende vast te leggen:

- De doelen van de onderzoeken;
- Alle verstrekkingen of doorgiften van politiegegevens;
- De doeleinden voor artikel 9 onderzoeken (zie ook Bijlage 3 – Wettelijke grondslagen voor het verwerken van persoonsgegevens);
- Feitelijke of juridische redenen die ten grondslag liggen aan een afwijzing van een inzageverzoek;
- Datalekken.

Deze documentatieplicht is geborgd in BRS.

2.16 Noodzakelijkheid, rechtmatigheid, vermelding herkomst en doelbinding

Politiegegevens worden alleen verwerkt als dat nodig is voor de in de wet genoemde doeleinden.

Het waterschap borgt dat politiegegevens niet op een onrechtmatige wijze worden verwerkt en dat er altijd sprake is van doelbinding. De herkomst van gegevens voor artikel 9 verwerkingen wordt altijd vermeld.

Hiervoor gelden deze maatregelen:

1. Politiegegevens worden slechts verwerkt voor zover dit noodzakelijk is voor de bij of krachtens de Wpg geformuleerde doeleinden.
2. Politiegegevens worden slechts verwerkt voor zover dit behoorlijk en rechtmatig is, de gegevens rechtmatig zijn verkregen en de gegevens, gelet op de doeleinden waarvoor zij worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.
3. Politiegegevens die zijn verkregen voor een doel, kunnen worden verwerkt voor een ander doel, voor zover deze Wpg uitdrukkelijk daarin voorziet en de verwerking voor dat andere doel noodzakelijk is en in verhouding staat tot dat doel.

4. Politiegegevens kunnen voor een ander doel worden verwerkt door personen en instanties die bij of krachtens de Wpg met het oog op een zwaarwegend algemeen belang of wetgeving van de Europese Unie zijn aangewezen.
5. Bij de verwerking van politiegegevens op grond van de artikelen 9 en 10 worden de herkomst van deze gegevens en de wijze van verkrijging vermeld.

Het waterschap voert aantoonbaar periodiek controles uit of vast te stellen of de bovenstaande maatregelen worden gevolgd.

Ten minste jaarlijks controleert de FG de dossiers en verwerkingen op noodzaak, rechtmatigheid en doelbinding.

2.17 Proportionaliteit, noodzakelijkheid en subsidiariteit

Voor alles wat je met politiegegevens doet, geldt dat je moet beoordelen of:

- 1) De verwerking in verhouding staat tot het doel dat je hebt (**proportionaliteit**);
- 2) Alle gegevens daadwerkelijk noodzakelijk zijn (**noodzakelijkheid**);
- 3) Je het doel kunt bereiken op een manier, die minder inbreuk maakt op de privacy van betrokkenen (**subsidiariteit**).

2.18 Juistheid en volledigheid politiegegevens

Het waterschap ziet toe dat de verwerkingsverantwoordelijke procedures heeft opgesteld en controles heeft ingericht op de kwaliteit ten behoeve van de borging van de juistheid en nauwkeurigheid van politiegegevens. Daarnaast zijn er procedures opgesteld voor het vernietigen en rectificeren van politiegegevens.

Hiervoor gelden deze maatregelen:

1. Het opnemen van maatregelen als gegevens onjuist worden verstrekt.
2. Het opnemen van maatregelen t.b.v. borging van juistheid en volledigheid.
3. Het inrichten van de maatregelen t.b.v. juistheid en volledigheid.
4. Het inrichten van de maatregelen t.b.v. onjuist verstrekte gegevens.
5. Het zichtbaar toezichthouden door de FG voor de Wpg op juistheid en volledigheid.

2.19 Onderscheid feiten en persoonlijk oordeel

Het waterschap ziet toe dat organisatorische en technische maatregelen zijn ingericht om politiegegevens die op feiten zijn gebaseerd, voor zover mogelijk, te onderscheiden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd

2.20 Boetes

Het niet of niet juist naleven van de Wpg, kan leiden tot een boete van de Autoriteit Persoonsgegevens (AP). De AP kan ook andere maatregelen opleggen, zoals een last onder dwangsom, een verwerkingsverbod, een berisping of een waarschuwing.

Naast de basisboete kan de boete worden aangepast op basis van verschillende factoren, zoals de aard en ernst van de overtreding, de getroffen maatregelen om de schade te beperken, en de mate van samenwerking met de toezichthouder.

3 Organisatie van beschermen van politiegegevens

In Paragraaf 2.5 Rollen, zijn de specifieke rollen voor de Wpg benoemd (De FG, de Bevoegd Functionaris en de BOA). Naast deze specifieke Wpg rollen hebben ook andere functies binnen de organisatie verantwoordelijkheden in het kader van de Wpg.

Deze verantwoordelijkheden voor het verwerken van persoonsgegevens conform wet- en regelgeving zijn in de tabel hieronder opgenomen.

Functie	Verantwoordelijkheden in het kader van de Wpg
Verwerkingsverantwoordelijke	• Is de (rechts)persoon die het doel en de middelen bepaalt voor de verwerking van politiegegevens. Voor een BOA is het de werkgever van de BOA, het Waterschap. • De verwerkingsverantwoordelijke is eindverantwoordelijk voor de naleving van de Wpg en zorgt ervoor dat: - het Wpg-beleid wordt vastgesteld en uitgevoerd; - de systemen worden aangepast; - de autorisaties goed geregeld zijn; - de beveiliging op orde is; - dat gegevens verwijderd en gedeeld worden; - dat audits en risicobeoordelingen worden gecoördineerd.
Verwerker	• Is de (rechts)persoon die politiegegevens verwerkt voor een verwerkingsverantwoordelijke.
Dagelijks Bestuur	• Het dagelijks bestuur is in de meeste gevallen verwerkingsverantwoordelijke voor de verwerking van persoons- en politiegegevens bij het waterschap. • Het dagelijks bestuur is eindverantwoordelijke voor het prioriteren van de uitvoering van het Wpg-beleid en het beschikbaar stellen en houden van voldoende middelen en capaciteit ten behoeve van de uitvoering van het privacy en Wpg-beleid.
Secretaris Directeur	• De secretaris-directeur is verantwoordelijk voor invoering en naleving van de Wpg wetgeving.
Manager	• Leidinggeven aan afdelingen die betrokken zijn bij de verwerking van politiegegevens. De manager is verantwoordelijk voor: - Naleven van de werkafspraken en instructies met betrekking tot de Wpg; - Zorgen voor correcte en veilige verwerking van politiegegevens; - Rapporteren van incidenten en gegevenslekken.
Privacy Officer	• Coördineren van projectmanagementactiviteiten met betrekking tot Wpg-naleving. De privacy Officer is het eerste aanspreekpunt voor de Wpg binnen het waterschap. De PO coördineert activiteiten en werkt daartoe samen met de FG, CISO, privacy jurist, BOA, Bevoegd Functionaris, managers en waar nodig met andere medewerkers.
Applicatiebeheerder	• Beheren van IT-systemen die worden gebruikt voor de verwerking van politiegegevens. De applicatiebeheerder is verantwoordelijk voor: - Implementeren en onderhouden van technische beveiligingsmaatregelen; - Toezicht houden op de toegang tot en het gebruik van applicaties; - Uitvoeren van periodieke controles en audits van systemen; - Rapporteren van technische incidenten en kwetsbaarheden.
Functioneel beheerder	• Beheren van documentatie en archivering van politiegegevens. De is verantwoordelijk voor: - Zorgen voor correcte archivering en vernietiging van politiegegevens volgens de Wpg; - Beheren van toegangsrechten tot archieven; - Uitvoeren van periodieke controles van archiefsystemen; - Rapporteren van afwijkingen in archiveringsprocessen.

Interne auditor	• Toezichthouder op algehele informatiebeveiliging binnen de organisatie. De interne auditor is verantwoordelijk voor: - Evalueren van de effectiviteit van Wpg-processen en procedures; - Identificeren van zwakke punten en doen van aanbevelingen voor verbetering; - Rapporteren van auditbevindingen aan de verwerkingsverantwoordelijke; - Volgen van de implementatie van aanbevolen verbeteringen.
CISO (Chief Information Security Officer)	• Toezichthouder op algehele informatiebeveiliging binnen de organisatie. De CISO is verantwoordelijk voor: - Toezicht houden op de naleving van de Wpg. - Adviseren over beveiligingsrisico's en mitigatiestrategieën.
Privacydesk	• Centraal aanspreekpunt voor privacy- en Wpg-gerelateerde vragen. De Privacydesk is verantwoordelijk voor: - Beantwoorden van vragen en verstrekken van informatie over de Wpg; - Ondersteunen bij nalevingsinitiatieven; - Coördineren van bewustwordingscampagnes; - Documenteren van privacy- en gegevensbeschermingsactiviteiten.
Juridische medewerker	• Verstrekken van juridische ondersteuning met betrekking tot Wpg-naleving. De Juridische Medewerker is verantwoordelijk voor: - Adviseren over juridische aspecten van gegevensverwerking; - Het ondersteunen van de proceseigenaar bij het opstellen en beoordelen van verwerkersovereenkomsten; - Vertegenwoordigen van de organisatie in juridische procedures; - Bijdragen aan de ontwikkeling en implementatie van beleid en procedures voor gegevensbescherming.

4 Controle, naleving

4.1 Controles

Self-assessments en veiligheidscontroles ten aanzien van de effectiviteit van de geïmplementeerde maatregelen ter beveiliging van persoonsgegevens worden uitgevoerd onder verantwoordelijkheid van de proceseigenaren van het waterschap. Verbeterpunten die naar aanleiding van deze controles worden vastgesteld, zijn onderdeel van de planning in de reguliere PDCA cyclus van de organisatie.

Geconstateerde afwijkingen worden als incident in het incident registratiesysteem vastgelegd, afgehandeld en gerapporteerd.

De volgende controles worden uitgevoerd:

Controle	Frequentie	Toelichting
Toegangscontrole & autorisatie	Jaarlijks	Controle of alleen bevoegde medewerkers toegang hebben tot politiegegevens.
Logging van toegang	Continu	Elke raadpleging van politiegegevens wordt automatisch vastgelegd.

Controle van logbestanden	Minimaal 1x per kwartaal	Controle van logbestanden om ongeoorloofd gebruik te detecteren.
Automatische logging van gebruik	Continu	Alle bewerkingen (inzage, mutatie, verstrekking) worden automatisch gelogd.
Steekproefsgewijze controle logbestanden	Minimaal 1x per kwartaal	Steekproefsgewijs wordt gecontroleerd of logregistraties correct en rechtmatig zijn.
Encryptie en netwerkbeveiliging	Jaarlijks	Controleer of politiegegevens versleuteld zijn en via beveiligde netwerken worden verzonden.
Beveiligingsupdates en patches	Minimaal maandelijks	Controle of beveiligingsupdates en patches tijdig zijn geïnstalleerd om kwetsbaarheden te dichten.
Penetratietesten / ethical hacking	Minimaal 1x per jaar	Een onafhankelijke partij voert jaarlijkse penetratietesten uit om beveiligingslekken te identificeren.
Controle op tijdige en correcte verwijdering	Minimaal 1x per jaar	Steekproefsgewijze controle of gegevens tijdig en correct zijn verwijderd (echt niet meer toegankelijk zijn).
Handmatige controle op datakwaliteit	Minimaal 1x per kwartaal	Controle of politiegegevens juist, actueel en relevant zijn voor het doel.
Controle op rechtmatigheid van verstrekkingen	Minimaal 1x per kwartaal	Er wordt steekproefsgewijs gecontroleerd of gegevens alleen rechtmatig worden gedeeld.
Beveiligde communicatiekanalen checken	Minimaal 1x per jaar	Beveiligde communicatiekanalen worden jaarlijks gecontroleerd op de actualiteit van de software- en beveiligingsupdates.
Controle van het verwerkingsregister	Minimaal 1x per jaar	Het verwerkingsregister wordt jaarlijks gecontroleerd op juistheid en volledigheid.
Interne audits	1x per jaar	Intern evalueren de naleving van de Wpg. Zie ook 4.2 Audits.
Externe audits	Elke 4 jaar	Externe controle op de naleving van de Wpg. Zie ook 4.2 Audits.

4.2 Audits

Binnen het waterschap worden in het kader van kwaliteitsmanagement periodiek in- en externe audits uitgevoerd op informatiebeveiligingsaspecten, waaronder ook de beveiliging van politiegegevens.

Jaarlijks wordt er een interne audit uitgevoerd. Elke vier jaar vindt een externe audit plaats.

Naar eigen inzicht van het waterschap kunnen er ook op ad hoc basis interne of externe audits worden uitgevoerd. Verbeterpunten die naar aanleiding van interne en/of externe audits worden vastgesteld, worden onderdeel van de reguliere rapportagecyclus.

De interne en externe auditor voeren de Wpg-audit uit aan de hand van de handreiking van NOREA⁴. Daarin staat een richtlijn 3000-D normenkader van normen die de externe auditor over een periode van 4 jaar toetst. Voor veel normen uit dit normenkader is het echter niet wenselijk en soms zelfs onmogelijk, om deze over de cyclus van 4 jaar te toetsen.

Dit betekent dat niet ieder jaar alle normen getoetst hoeven te worden. Wel is verplicht dat uiteindelijk in die 4 jaar alle normen over een periode van 12 maanden zijn getoetst.

In de NOREA handreiking zijn 7 normen als toezicht maatregelen aangeduid.

Deze toezicht maatregelen moeten wel over de gehele cyclus van 4 jaar toetsen.

Het is daarom belangrijk om deze toezicht maatregelen ook tijdens iedere jaarlijkse interne audit te toetsen:

⁴ Zie deze link: <https://www.norea.nl/uploads/bfile/c97a8a0c-0b10-4be7-a10e-be3c041b9f2d> en voor de herbeoordeling deze link: <https://www.norea.nl/uploads/bfile/963a9e81-7c4e-4526-a766-8c0d5f52cb38>

1. Jaarlijks toezicht van de FG op de doelbinding.
2. Controles op de noodzakelijkheid en rechtmatigheid door de FG (of PO).
3. Controles op het vernietigen en rectificeren van politiegegevens.
4. Controles op uitvoering DPIA's.
5. Beschikbaarheid logbestanden.
6. Planning, uitvoering en rapportage van de interne audits.
7. Overige toezichttaken van de FG.

5 Bijlagen

5.1 Bijlage 1 – Afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene verordening gegevensbescherming
BF	Bevoegd Functionaris
BIO	Baseline Informatiebeveiliging Overheid
BOA	Buitengewoon opsporingsambtenaar
BRS	BOA Registratie Systeem
BSN	Burgerservicenummer
CIP	Centrum Informatiebeveiliging en Privacybescherming
CISO	Chief Information Security Officer
CPW	Coördinatorenoverleg Privacy Waterschappen
DPIA	Data Protection Impact Assessment of gegevensbeschermingseffectbeoordeling
FG	Functionaris gegevensbescherming
GEB	Gegevensbeschermingseffectbeoordeling of DPIA
Wpg	Wet politiegegevens

5.2 Bijlage 2 – Belangrijke definities

„Persoonsgegevens”:

alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

„Verwerking”:

een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

„Verwerkingsverantwoordelijke”:

een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoons- dan wel politiegegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;

„Verwerker”:

een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoons- dan wel politiegegevens verwerkt;

„Inbreuk in verband met persoonsgegevens of politiegegevens” ("datalek"):

een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;

„Politiegegevens”:

Politiegegevens zijn alle gegevens die door of voor een politie-instantie worden verwerkt voor de

uitvoering van de politietaak. Deze gegevens zijn specifiek bedoeld voor het voorkomen, opsporen, onderzoeken en vervolgen van strafbare feiten en voor het handhaven van de openbare orde. De Wet politiegegevens (Wpg) legt de nadruk op het verwerken van deze gegevens op een wijze die de privacy van individuen beschermt, terwijl het mogelijk maakt om effectief politiewerk te verrichten.

Kenmerken van Politiegegevens:

1. **Specifiek Doel:**
Politiegegevens worden verzameld en verwerkt voor duidelijk gedefinieerde politietaken. Dit omvat activiteiten zoals criminaliteitsbestrijding, handhaving van de openbare orde, en het bieden van hulp bij noodsituaties.
2. **Gevoelig Karakter:**
Deze gegevens kunnen zeer gevoelig zijn en betrekking hebben op strafrechtelijke feiten, verdenkingen, en andere informatie die relevant is voor politieonderzoeken.
3. **Beperkte Toegang:**
Toegang tot politiegegevens is strikt gereguleerd en beperkt tot diegenen die deze gegevens nodig hebben voor de uitvoering van hun politietaken.
4. **Bewaartermijnen:**
De Wpg stelt specifieke bewaartermijnen vast voor politiegegevens, waarbij gegevens niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor ze zijn verzameld.
5. **Verwerking en Beveiliging:**
De verwerking van politiegegevens moet voldoen aan strenge beveiligingsmaatregelen om de integriteit, vertrouwelijkheid en beschikbaarheid van de gegevens te waarborgen.

Voorbeelden van Politiegegevens:

- **Strafrechtelijke Verleden:**
Informatie over eerdere veroordelingen en strafbare feiten.
- **Onderzoekgegevens:**
Gegevens verzameld tijdens lopende politieonderzoeken, zoals getuigenverklaringen en bewijsmateriaal.
- **Opsporingsinformatie:**
Gegevens over personen die worden verdacht van betrokkenheid bij strafbare feiten.
- **Incidentrapportages:**
Verslagen van incidenten die de politie heeft afgehandeld, zoals meldingen van geweld, diefstal, of overlast.

Door het zorgvuldig beheren en beveiligen van politiegegevens, draagt het waterschap bij aan het waarborgen van zowel de privacy van individuen als de effectiviteit van politietaken. De Wpg biedt een duidelijk kader voor hoe deze gevoelige gegevens op een verantwoordelijke en wettelijk conforme manier moeten worden behandeld.

5.3 Bijlage 3 – Wettelijke grondslagen voor het verwerken van persoonsgegevens

De AVG kent zes grondslagen voor de verwerking van persoonsgegevens.

Een verwerking van persoonsgegevens voor AVG moet minimaal op één van de zes grondslagen zijn gebaseerd.

De Wpg heeft een andere invalshoek. De Wpg stelt dat de verwerking van politiegegevens gebaseerd moet zijn op een noodzakelijke grondslag die specifiek verband houdt met de uitvoering van de politietaak.

Daarnaast kent de Wpg drie verwerkingsgrondslagen waarvan er (tot op heden) slechts twee op de (BOA's van de) waterschappen van toepassing zijn. Dit zijn de volgende grondslagen:

Artikel 8: Dagelijkse politietaak

Persoonsgegevens die verwerkt worden in het kader van de dagelijkse opsporingstaak, vallen onder artikel 8 van de Wpg. Dit gaat over zaken als foutief aanbieden van afval maar ook het proces verbaal opmaken bij onrechtmatig afgeschoten wild of tuinafvaldump.

Artikel 9: Gerichte verwerkingen

Dit artikel 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 opsporingsbevoegd heden

worden ingezet, zoals het plaatsen van een baken onder een auto bij verdenking van stroperij of stelselmatige observatie bij verdenking van een milieudelict.

Nota bene: Artikel 13 Ondersteunende taken is niet op het waterschap van toepassing.

Het waterschap verwerkt alleen persoonsgegevens als daar een wettelijke grondslag voor is. In onderstaande tabel zijn de grondslagen van de AVG en de Wpg met elkaar vergeleken.

Verwerkingsgrondslag	AVG	Wpg
Toestemming	De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden.	Niet van toepassing.
Uitvoering van een overeenkomst	Verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen.	Niet van toepassing.
Wettelijke verplichting	Verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.	Verwerking is noodzakelijk voor de uitvoering van een wettelijke verplichting van de politie of andere opsporingsdiensten. In praktijk verwijst dit naar artikel 8 van Wpg.
Vitaal belang	Verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen.	Verwerking is noodzakelijk voor de bescherming van de vitale belangen van de betrokkene of van anderen.
Algemeen belang en uitoefening van openbaar gezag	Verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.	Verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang in het kader van de politietaak. In praktijk verwijst dit naar artikel 8 van Wpg.
Gerechtvaardigd belang	Verwerking is noodzakelijk voor de doeleinden van de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke of door een derde worden nagestreefd, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die bescherming van persoonsgegevens vereisen, zwaarder wegen dan die belangen.	Niet van toepassing.
Artikel 8 Wpg	Niet van toepassing.	Politiegegevens worden verwerkt voor de uitvoering van de politietaak zoals bedoeld in artikel 8 van de Wpg.

Artikel 9 Wpg	Niet van toepassing.	Verwerking van politiegegevens voor andere dan de in artikel 8 genoemde doeleinden, mits voldaan wordt aan aanvullende voorwaarden zoals vastgelegd in artikel 9 van de Wpg.
----------------------	----------------------	--

5.4 Bijlage 4 – Bewaartermijnen Wpg

Afhankelijk van de grondslag van de verwerking van politiegegevens worden de onderstaande bewaartermijnen gehanteerd.

Grondslag	Doel	Verwerking	Termijnen	Vernietiging
Artikel 8	Dagelijkse boa-taak	Verzamelen van persoonsgegevens voor dagelijkse werkzaamheden zoals wildplassen, afvalbeheer, alcoholgebruik op openbare weg en loslopende honden.	Gegevens mogen tot vijf jaar na de eerste verwerkingsdatum worden benaderd.	Gegevens worden vijf jaar na de eerste verwerking verwijderd en daarna bewaard voor vijf jaar voor audits of klachten.
Artikel 9	Gerichte verwerkingen	Specifieke gegevensverwerkingen gericht op bepaalde personen of gebeurtenissen, bijvoorbeeld onderzoeken met bijzondere opsporingsbevoegdheden.	Gegevens worden verwijderd zodra ze niet meer nodig zijn of maximaal zes maanden verwerkt voor herbruikbaarheid.	Verwijderde gegevens worden vijf jaar bewaard en vervolgens vernietigd.

5.5 Bijlage 5 – Geraadpleegde bronnen

- [Wet politiegegevens](#),
- [Algemene verordening Gegevensbescherming](#), 27 april 2016, Europees Parlement
- [Uitvoeringswet Avg](#)
- [Praktijkhandboek Wpg](#), Suzanne Franken, september 2023
- Handboek Handhaving, Waterschap De Dommel, 1 februari 2024
- Plan van aanpak Wpg versie 2, Waterschap De Dommel
- BIO Risicoassessment Informatieveiligheid en Privacy Wpg v1.0, Waterschap Aa en Maas
- DPIA BRS v1.2
- NOREA Handreiking Privacy audit Wpg voor boa's versie 2024 1.0, 3 september 2024
- FAQ – Privacy Audit Wpg versie 1, NOREA, 17 november 2021
- [De 10 dingen die je wilt weten over de Wpg - Verdonck, Klooster & Associates \(vka.nl\)](#)