hoogheemraadschap Hollands Noorderkwartier

WATERSCHAPSBLAD

Officiële uitgave van het dagelijks bestuur van het Hoogheemraadschap Hollands Noorderkwartier

Nr. 21902
12 september 2025

Privacybeleid HHNK 2025-2027

1 Inleiding

Het Hoogheemraadschap Hollands Noorderkwartier (hierna: het hoogheemraadschap of HHNK) werkt met (persoons)gegevens van burgers, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt het hoogheemraadschap om de wettelijke taken goed uit te kunnen voeren. Denk hierbij aan taken zoals het heffen en innen van waterschapsbelasting en het opmaken van proces verbaal door onze buitengewoon opsporingsambtenaren. Om deze taken goed te volbrengen is het noodzakelijk dat het hoogheemraadschap persoonsgegevens verwerkt. Verwerking van persoonsgegevens is een breed begrip, bijna alles wat je met persoonsgegevens doet valt onder verwerken. Handelingen die er in ieder geval onder vallen, zijn: het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen en vernietigen van gegevens. De burger moet erop kunnen vertrouwen dat het hoogheemraadschap zorgvuldig en veilig met deze persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. Het hoogheemraadschap is zich hiervan bewust en geeft daarom met dit beleid aan hoe het in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van de bescherming van persoonsgegevens, waaronder de Algemene Verordening Gegevensbescherming (hierna: AVG) en de Wet Politiegegevens (hierna: Wpg).

Geldigheidsduur
Dit beleid is vastgesteld op 26 augustus 2025 door het college van dijkgraaf en hoogheemraden (hierna: D&H) als eindverantwoordelijke voor de gegevensverwerking. Het beleid wordt in lijn met het AVG-normenkader tenminste eens per drie jaar beoordeeld en zo nodig herzien. Indien daar aanleiding toe is kan het D&H besluiten tot een tussentijdse herziening.

2 Begripsbepalingen

De definities van artikel 4 AVG en artikel 1 Wpg (hierna: privacywetgeving) worden in dit beleidsdocument gevolgd.

3 Reikwijdte

Het hoogheemraadschap verzamelt en gebruikt persoonsgegevens van inwoners, leveranciers en medewerkers en andere natuurlijke personen (hierna te noemen: betrokkenen).

Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens het hoogheemraadschap, waaronder:
1. De verwerking van persoonsgegevens binnen de bedrijfsprocessen van het hoogheemraadschap;
2. De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd;
3. De gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden of leveranciers.

Dit privacybeleid is van toepassing op de verwerkingen van persoonsgegevens die vallen onder de AVG de Wpg. Voor informatie over de verantwoordelijkheden rondom de uitvoering en borging van dit beleid, zie hoofdstuk 7 'Rollen en verantwoordelijkheden' en hoofdstuk 11 'RASCI-tabel'.

4 Doel

Met dit privacybeleid geeft het hoogheemraadschap een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van de personen waarvan het hoogheemraadschap persoonsgegevens verwerkt (of laat verwerken).

Daarnaast beoogt dit privacybeleid taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens verder af te bakenen en aan te scherpen.

De verdere uitwerking van dit beleid is - waar relevant - vastgelegd in de operationele documenten binnen het hoogheemraadschap, zoals standaarden, procedures, richtlijnen, privacy-verklaringen en domeinspecifiek privacybeleid.

Naast dit door het D&H vastgestelde privacybeleid is een Informatieveiligheidsbeleid HHNK 2025-2027 vastgesteld. Hierin zijn maatregelen opgenomen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens. Het privacybeleid kan daarom niet los worden gezien van het informatieveiligheidsbeleid. Dit informatieveiligheidsbeleid is vastgesteld door het D&H van het hoogheemraadschap.

5 Visie en ambitie

De komende jaren zet het hoogheemraadschap in op het verder verhogen van de privacybewustwording en professionalisering van de privacy functie in de organisatie. Een goede privacy boekhouding is noodzakelijk voor het goed functioneren van het hoogheemraadschap en de basis voor het beschermen van rechten van burgers, medewerkers en bedrijven. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Daarbij is verantwoord en bewust gedrag van alle medewerkers essentieel voor de bescherming van persoonsgegevens binnen het hoogheemraadschap. Iedere medewerker wordt daarom aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via werkinstructies. Dit gebeurt passend binnen de context van en bij het organisatieonderdeel waarbinnen die worden verwerkt.

Privacy kent aanknopingspunten met ander beleid in de organisatie. Denk bijvoorbeeld aan archiefbeleid, personeelsbeleid, informatieveiligheidsbeleid en fysiek en sociaal veiligheidsbeleid. Dit beleid moet op elkaar aansluiten en waar nodig naar elkaar verwijzen. Beleidsdocumenten over andere onderwerpen zijn in lijn met dit privacybeleid.

Mede in het kader van de visie op veiligheidscultuur van HHNK, is een goede afstemming tussen de aangrenzende beleidsterreinen voortdurend nodig. Gezien de sterke verwevenheid van de beleidsterreinen kiest HHNK zoveel mogelijk voor een uniforme en integrale aanpak.

5.1.1 Verwerkingen die vallen onder de AVG

Er zijn vijf volwassenheidsniveau 's voor de bescherming van persoonsgegevens die vallen onder AVG. Om aan de AVG te voldoen is in ieder geval een zogenaamd beheerst niveau nodig. Het hoogheemraadschap heeft zich in 2019 als doel gesteld om in 2024 een volwassenheidsniveau 4 te realiseren volgens het AVG-normenkader. Dat betekent dat het hoogheemraadschap aantoonbaar voldoet aan de AVG-normen en dat deze geborgd zijn in een Plan-Do-Check-Act-cyclus (hierna: PDCA-cyclus). Het hoogheemraadschap heeft daarom de ambitie om naar dat niveau door te groeien en maatregelen te treffen om vervolgens dat niveau te behouden. Een uitleg per volwassenheidsniveau is opgenomen in onderstaande tabel 1.

Volwassenheid privacy beleidsvoering		
	Niveau	Omschrijving
5	**Geoptimaliseerd**	• Proactieve houding van het college en het bestuur • Het verantwoordelijk management verzoekt aan de Functionaris Gegevensbescherming (hierna: FG) om hun verantwoording van een oordeel te voorzien • Privacy wordt gezien als een vanzelfsprekendheid • Er wordt continue gezocht naar verbetering, zoals in de vorm van (interne of externe) tooling • Privacy wordt gezien als een kans of unique selling point (USP) • Er wordt verbinding gezocht met andere concerndisciplines • Kennis en ervaringen worden actief gedeeld met Waterschappen en andere relevante organisaties waardoor best practices ontstaan • Onbewust bekwaam
4	**Beheerst**	• De effectiviteit van beheersmaatregelen wordt periodiek geëvalueerd in een PDCA-cyclus • Er wordt proactief geïnformeerd door de proceseigenaar over de realisering van de geconstateerde benodigde verbeteringen in een PDCA-cyclus • In een jaarlijkse evaluatie blijkt een correcte PDCA-cyclus • Bewust bekwaam

3	**Bepaald**	• (Privacy)medewerkers tonen eigenaarschap, d.w.z. dat de rollen en verantwoordelijkheden actief worden opgepakt • Er wordt aantoonbaar aan verplichtingen voldaan • Verwerkingsverantwoordelijke bestuursorganen nemen beslissingen mede op grond van risicoanalyses zoals een Data Protection Impact Assessment (hierna: DPIA) • Er is een duidelijke samenhang met informatiebeveiliging • Bewust bekwaam
2	**Herhaalbaar**	• Privacy rollen en -verantwoordelijkheden toegewezen • Beheersmaatregelen zijn aanwezig, maar worden op informele wijze uitgevoerd • Standaarden en formats aanwezig: juist en in duidelijke taal • Bewust onbekwaam
1	**Ad hoc**	• Geen of onduidelijke privacy rollen en -verantwoordelijkheden • Geen of nauwelijks beheersmaatregelen aanwezig • Reactief en sturing n.a.v. incidenten • Grote afhankelijkheid van één of enkele privacyfunctionarissen • Onbewust onbekwaam

Tabel 1

5.1.2 Verwerkingen die vallen onder de Wpg

In de Wpg zijn vereisten en regels opgenomen voor het verwerken van persoonsgegevens die nodig zijn om de opsporing van strafbare feiten goed te kunnen uitvoeren. De Wpg zorgt daarbij voor een evenwicht tussen de belangen die met het uitvoeren van de opsporing van strafbare feiten gemoeid zijn en het beschermen van de privacy van burgers.

De Wpg verdeelt de verwerking voor opsporing van strafbare feiten in zes domeinen. Het hoogheemraadschap verwerkt persoonsgegevens voor de opsporing van strafbare feiten in domein II dat betrekking heeft op Milieu, Welzijn en infrastructuur. Voor de opsporing van strafbare feiten heeft het hoogheemraadschap speciaal daarvoor bevoegde Buitengewoon Opsporingsambtenaren (hierna: boa's) aangesteld.

De Wpg heeft wettelijke normen waaraan moet worden voldaan. Om aan de Wpg te voldoen geldt dat voor al die normen opzet, bestaan en werking moet worden aangetoond.

Opzet	De organisatie heeft de beheersingsmaatregen beschreven die, indien deze werken zoals beschreven, een redelijke mate van zekerheid bieden dat voorzien is aan de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's.
Bestaan	De organisatie heeft de beheersingsmaatregelen overeenkomstig de opzet daadwerkelijk geïmplementeerd en toegepast.
Werking	De organisatie heeft de beheersingsmaatregelen gedurende de verslaggevingsperiode volgens de opzet toegepast; ingeval van handmatige beheersingsmaatregelen zijn deze toegepast door competente en bevoegde personen.

De Wpg werkt niet met volwassenheidsniveau 's. Als voor het domein wordt voldaan aan opzet, bestaan en werking komt dat overeen met het volwassenheidsniveau 4 van de AVG. Het hoogheemraadschap heeft daarom de ambitie om naar dat niveau door te groeien en maatregelen te treffen om vervolgens dat niveau te behouden.

5.1.3 Telecommunicatiewet

Naast de AVG en Wpg is de Telecommunicatiewet van toepassing. De Telecommunicatiewet is de wettelijk verankering van omgang met cookies en daarom voor het hoogheemraadschap van belang.

6 Principes voor de verwerking van persoonsgegevens

De AVG en de Wpg zijn gebaseerd op een aantal principes voor de verwerking van persoonsgegevens. Het hoogheemraadschap onderschrijft deze principes en stelt zich ten doel persoonsgegevens slechts te verwerken in overeenstemming met deze principes. Hieronder worden deze principes puntsgewijs besproken.

6.1.1 Rechtmatige grondslag
Persoonsgegevens worden door het hoogheemraadschap slechts verwerkt in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze. Dit betekent onder meer dat verwerkingen alleen plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking bij het hoogheemraadschap voort uit een wet (wettelijke verplichting) of een publiekrechtelijke taak.

6.1.2 Welbepaalde doeleinden
Het hoogheemraadschap verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen. Dit betekent dat het hoogheemraadschap alleen die persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken (ter zake dienend). Het hoogheemraadschap ziet af van de verwerking als het doel op een andere – minder ingrijpende – wijze kan worden bereikt, bijvoorbeeld door minder of geen persoonsgegevens te verwerken.

6.1.3 Verdere verwerking (doelbinding)
Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor deze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. Het hoogheemraadschap voert, voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

6.1.4 Minimale gegevensverwerking
Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiest het hoogheemraadschap voor die mogelijkheid. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een wijze kan worden verwezenlijkt die minder inbreuk maakt op de privacy van de betrokkene, dan kiest het hoogheemraadschap voor die mogelijkheid.

6.1.5 Juiste en actuele gegevens
Het hoogheemraadschap zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn gelet op het doel waarvoor zij verzamelt zijn of vervolgens worden verwerkt. Het hoogheemraadschap neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden.

6.1.6 Gegevens worden op tijd vernietigd
Het hoogheemraadschap stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en – voor zover het verwerkingen betreft die vallen onder de AVG - de selectielijst. Waterschappen – waaronder het hoogheemraadschap - hebben op grond van de Archiefwet onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard.

Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt het hoogheemraadschap de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. Het hoogheemraadschap bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is. Nadere regels ten aanzien van het bewaren en vernietigen zijn opgenomen in de standaard bewaren en vernietigen.

6.1.7 Integriteit en vertrouwelijkheid
Het hoogheemraadschap neemt passende technische en organisatorische maatregelen om de persoonsgegevens, met name bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. Het hoogheemraadschap handelt hierbij in overeenstemming met het informatieveiligheidsbeleid. Het informatieveiligheidsbeleid verplicht het hoogheemraadschap om informatie te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking.

Het hoogheemraadschap houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van persoonsgegevens. Dit uitgangspunt wordt *Privacy by Design* genoemd. Het hoogheemraadschap draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt het hoogheemraadschap *Privacy by Default* als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

Uitsluitend geautoriseerde gebruikers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend. Deze bevoegdheden worden verleend op grond van het binnen het hoogheemraadschap geldend beleid voor toegang tot gegevens, waaronder het informatieveiligheidsbeleid. Het beheer van bevoegdheden wordt periodiek gecontroleerd, door de hoofd/proceseigenaar zoals omschreven in paragraaf 7.1.6. Het hoogheemraadschap hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens, om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

6.1.8 Inbreuk in verband met persoonsgegevens
Bij toegang tot, verlies of wijziging van persoonsgegevens bij het hoogheemraadschap, zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet, afhankelijk van het risico, worden gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens) en soms bij de getroffen betrokkenen. Het hoogheemraadschap registreert datalekken, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in de standaard datalekken.

6.1.9 Advies inwinnen bij privacy officer
Alvorens aangevangen wordt met een nieuwe of verdere verwerking van persoonsgegevens wint het management advies in bij de privacy officer. Regels ten aanzien van de afhandeling van adviesvragen zijn opgenomen in de standaard privacyadvies inwinnen.

6.1.10 Samenwerking
Het hoogheemraadschap schakelt soms derden in om persoonsgegevens in opdracht van het hoogheemraadschap te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacywetgeving en aan het privacybeleid van het hoogheemraadschap. De AVG en Wpg verplichten het hoogheemraadschap tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten. Daarin wordt geborgd dat de verwerker zich inderdaad aan de privacywetgeving en aan het privacybeleid van HHNK houdt. Nadere regels ten aanzien van het opstellen en vaststellen van verwerkersovereenkomsten zijn opgenomen in de standaard verwerkersovereenkomsten. In sommige gevallen is het hoogheemraadschap zelf verwerker van persoonsgegevens - dan gelden dezelfde regels.

6.1.11 Samenwerkingsverbanden
Verder kan het voorkomen dat het hoogheemraadschap samenwerkt met andere (overheids-)organisaties om een taak van algemeen belang uit te voeren. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). Het hoogheemraadschap maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat gelijk is aan dat van het hoogheemraadschap.

Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie, geschiedt alleen in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en dit privacybeleid.

6.1.12 Transparantie
Het hoogheemraadschap informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Alleen indien de wet anders bepaalt, wijkt het hoogheemraadschap van deze informatieplicht af.

Het hoogheemraadschap beschikt over een verwerkingsregister, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt. Nadere regels ten aanzien van het actueel houden van het verwerkingsregister zijn opgenomen in de standaard verwerkingsregister.

Iedereen heeft het recht om te vernemen welke persoonsgegevens het hoogheemraadschap over hem of haar heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit de wet uit te oefenen. Voor de AVG betreft dit het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking, recht op overdraagbaarheid en het recht op uitsluiting van geautomatiseerde verwerking. Voor de Wpg betreft dit het recht van inzage, recht op rectificatie/aanvulling, het recht op afscherming en het recht op vernietiging. Deze rechten zijn niet absoluut. Nadere regels ten aanzien van de rechten van betrokkenen zijn opgenomen in de standaard rechten van betrokkenen. Betrokkenen worden over hun rechten nader geïnformeerd via de privacyverklaring op de website van het hoogheemraadschap.

Indien de betrokkene van mening is dat het hoogheemraadschap niet op een juiste wijze met zijn of haar persoonsgegevens is omgegaan, kan hij of zij een klacht indienen door middel van de van toepassing zijnde klachtenprocedure zoals opgenomen in de privacyverklaring van het hoogheemraadschap. De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

6.1.13 Verantwoording
Als ambitie is geformuleerd dat het hoogheemraadschap aan de AVG en Wpg voldoet. Dat vereist dat het hoogheemraadschap *in control* is en daarover op professionele wijze verantwoording aflegt. *In control* betekent in dit verband dat het hoogheemraadschap weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een PDCA-cyclus.

Het hoogheemraadschap hanteert het *three lines* model bij het inrichten van de privacyorganisatie.

De eerste lijn bestaat uit het lijnmanagement en is verantwoordelijk voor het managen van de risico's, het vaststellen en accepteren van eventuele restrisico's en voor het borgen van de aantoonbare naleving van de wet- en regelgeving op het terrein van privacybescherming.

De tweede lijn bestaat uit de privacy officer en is verantwoordelijk voor het leveren van expertise, ondersteuning, monitoring en rapportage.

De derde lijn bestaat uit een FG en een interne auditor. De FG houdt intern bij het hoogheemraadschap toezicht op de naleving van de AVG en Wpg. De interne (IT-)auditor is verantwoordelijk voor de onafhankelijke, objectieve toetsing of in opzet, bestaan en werking wordt voldaan aan het wettelijke Wpg-normenkader en het geven van aanbevelingen.

De Security Board (als onderdeel van het directieoverleg) bestaat uit de directie, de afdelingshoofden HRVCF, CC, I&A, CISO en FG. Zij bespreken driemaandelijks de staat van informatieveiligheid en privacy naar aanleiding van incidenten, lopende zaken en rapportages over het realiseren en borgen van het gewenste beveiligingsniveau, rekening houdend met wet- en regelgeving en de organisatiedoelstellingen.

Als een verwerking mogelijk een hoog risico inhoudt voor de betrokkene, moet het hoogheemraadschap een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. Het hoogheemraadschap voert in dat geval een DPIA uit. Als uit de DPIA blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet het hoogheemraadschap voldoende maatregelen nemen om de risico's te verminderen. Als het niet lukt om (voldoende) maatregelen te nemen om dit risico te beperken, dan moet het hoogheemraadschap met de Autoriteit Persoonsgegevens overleggen, voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd. Nadere regels ten aanzien van de DPIA's zijn opgenomen in de standaard DPIA's van het hoogheemraadschap.

6.1.14 PDCA
Voor de AVG en Wpg is er een PDCA-cyclus. In een privacyjaarplan (als onderdeel van een Integraal Veiligheidsplan), de afdelingsplannen en een Wpg verbeterplan worden jaarlijks verbetermaatregelen opgesteld. Het Wpg verbeterplan geeft een overzicht van de verbetermaatregelen die de organisatie moet treffen om te voldoen aan de Wpg. Deze plannen worden periodiek geëvalueerd.

Het lijnmanagement informeert elk triaal de tweedelijns privacy officer over de voortgang van de uitvoering van privacyactiviteiten, zoals opgenomen in de jaarlijkse afdelingsplannen.
De tweedelijns privacy officer ondersteunt de organisatie bij het verwerken van persoonsgegevens conform het privacybeleid en rapporteert hierover aan management, FG, directie en bestuur. Deze rapportage vindt in ieder geval plaats in triaalrapportages 1 en 2 en bij de jaarrekening.

De FG ziet er als derdelijns functionaris op toe dat de AVG en de Wpg intern worden nageleefd. Het hoogheemraadschap stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.

De wijze waarop verder verantwoording wordt afgelegd is voor de AVG- en Wpg-verwerkingen verschillend. De FG rapporteert minimaal één keer per jaar zijn of haar bevindingen aan management, directie en bestuur over de naleving van de AVG en Wpg door het hoogheemraadschap. De FG baseert zijn of haar bevindingen mede op de triaalrapportages zoals aangeleverd door de privacy officer.

Ten aanzien van de verantwoording over de wijze waarop het hoogheemraadschap omgaat met de verwerking van persoonsgegevens rondom strafbare feiten bij handhavingstaken wordt vanuit de Wpg verplicht om iedere vier jaar een externe audit uit te laten voeren aan de hand van het wettelijke Wpg-normenkader. Op onderdelen waarop het hoogheemraadschap nog niet voldoet aan de wettelijke vereisten dient binnen drie maanden een verbeterrapport te worden opgesteld. Een hercontrole op de gedane verbeteringen dient dan binnen één jaar na de externe audit plaats te vinden. Tevens is het vanuit de Wpg verplicht om jaarlijks een interne audit uit te (laten) voeren naar de opzet, bestaan en werking van een (deel) van maatregelen uit het wettelijke Wpg-normenkader. In de interne audit worden ook de bevindingen uit de voorgaande audit getoetst op opvolging.

7 Rollen en verantwoordelijkheden

Een belangrijk uitgangspunt in privacywetgeving is de verantwoordingsplicht: het hoogheemraadschap is verantwoordelijk voor de naleving van de in privacywetgeving neergelegde eisen en kan aantonen dat het hieraan voldoet [1]. Om hieraan te kunnen voldoen dient binnen de organisatie sturing en monitoring plaats te vinden op naleving van privacywetgeving en dit privacybeleid. In dit hoofdstuk is beschreven hoe de bescherming van persoonsgegevens is belegd binnen de organisatie. In hoofdstuk 11 is een RASCI-tabel opgenomen dat overeenkomt met onderstaande rollen en verantwoordelijkheden.

7.1.1 Dagelijks Bestuur

Het dagelijks bestuur (DB), ook wel aangeduid als college van dijkgraaf en hoogheemraden (D&H), is eindverantwoordelijk voor de rechtmatige, zorgvuldige en transparante verwerking van persoonsgegevens binnen het hoogheemraadschap. Dit geldt ook voor de verwerking van persoonsgegevens die ter beschikking worden gesteld aan derden of worden gedeeld in samenwerkingsverbanden. Het DB stelt elke drie jaar in lijn met het AVG-normenkader het privacybeleid vast. Het DB bevordert de beschikbaarheid van voldoende middelen om uitvoering van het privacybeleid te waarborgen.

7.1.2 De secretaris-directeur

De verantwoordelijkheid van de secretaris-directeur valt uiteen in twee onderdelen.

Enerzijds is de secretaris-directeur op grond van de Mandaatregeling Hoogheemraadschap Hollands Noorderkwartier 2012 door het DB gemandateerd om beslissingen te nemen inzake de bescherming van persoonsgegevens. Overige bevoegdheden van het DB kunnen ook worden uitgeoefend door de secretaris-directeur, voor zover deze in mandaat aan hem zijn gegeven.

Anderzijds is de secretaris-directeur de hoogste ambtelijke eindverantwoordelijke op het gebied van privacy. De secretaris-directeur stelt zo nodig uitvoeringsmaatregelen vast ten behoeve van de bescherming van persoonsgegevens.

7.1.3 Directie

De directie bestaat uit de secretaris-directeur, de directeur bedrijfsvoering en de directeur water. De directie stelt het privacyjaarplan (als onderdeel van een Integraal Veiligheidsplan) vast. De directeur bedrijfsvoering is verantwoordelijk voor het aan- en bijsturen van de eerste en tweede lijn op het gebied van privacy. De directeur water is verantwoordelijk voor het aan- en bijsturen van de eerste lijn op het gebied van privacy.

De triaalrapportages, het jaarverslag privacy en de evaluatie van het beleid worden aan de directie gepresenteerd. De directie wordt periodiek in de Security Board geïnformeerd over ontwikkelingen op het gebied van informatieveiligheid en privacy en in staat gesteld te sturen op de realisatie van de doelstellingen en beheersing van de risico's.

7.1.4 Security Board

De Security Board (als onderdeel van het directieoverleg) bestaat uit de directie, de afdelingshoofden HRVCF, CC, I&A en de CISO en FG. Zij bespreken driemaandelijks de staat van informatieveiligheid en privacy naar aanleiding van incidenten, lopende zaken en rapportages omtrent het realiseren en borgen van het gewenste beveiligingsniveau, rekening houdend met wet- en regelgeving en de organisatiedoelstellingen.

7.1.5 De ambtenaar belast met de heffing en invordering

De ambtenaar belast met de heffing en invordering, zoals bedoeld in artikel 123, derde lid onderdelen b en c van de Waterschapswet, is aangewezen door het DB en heeft op grond van attributie diverse wettelijke bevoegdheden. De ambtenaar belast met de heffing en invordering is een bestuursorgaan

1) *Zie artikel 5 lid 2 AVG en artikel 33 Wpg*

en is zelf verantwoordelijk voor rechtmatige, zorgvuldige en transparante verwerking van persoonsgegevens ten behoeve van de heffing en invordering van waterschapsbelastingen. De ambtenaar belast met de heffing en invordering conformeert zich aan het door D&H vastgestelde beleid, uitvoeringsmaatregelen, standaarden, procedures en richtlijnen op het gebied van verwerkingen van persoonsgegevens.

7.1.6 Applicatie-eigenaar en gedelegeerd applicatie-eigenaar
Iedere applicatie eigenaar zorgt ervoor dat de applicatie aan de verwachtingen en eisen omtrent Beschikbaarheid, Integriteit, Vertrouwelijkheid en Privacy (BIVP) blijft voldoen, vandaag en in de toekomst. Deze bevoegdheid is niet 'absoluut' in die zin dat er ook gehoor moeten worden gegeven aan andere eisen dan voor IV&P, bijv. eisen voortkomend uit het Microsoft-tenzij-beleid of de architectuur-principes van HHNK.

De gedelegeerd applicatie eigenaar is verantwoordelijk voor de operationele taken die bij het functioneel beheer van een applicatie komen kijken.

Alvorens aangevangen wordt met een nieuwe of verdere verwerking van persoonsgegevens winnen de applicatie eigenaar en de gedelegeerd applicatie eigenaar advies in bij de privacy officer.

7.1.7 Afdelingshoofden/proceseigenaren
De hoofd/proceseigenaar heeft de bevoegdheid om te bepalen hoe een proces verloopt en heeft de verantwoordelijkheid om ervoor te zorgen dat het proces aan de verwachtingen en organisatiedoelen blijft voldoen, vandaag en in de toekomst.

Voor ieder primair of ondersteunend proces binnen het hoogheemraadschap is een hoofd/proceseigenaar aangewezen die zorgdraagt voor de vormgeving, uitvoering en monitoring van privacybeheersmaatregelen binnen zijn afdeling en verwerkingsproces en die aanspreekbaar is op het effectief waarborgen van privacy in dat proces. De hoofd/proceseigenaar stelt standaarden, procedures, privacyverklaringen en domeinspecifiek privacybeleid vast. De hoofd/proceseigenaar is verantwoordelijk voor de inrichting en uitvoering van de bedrijfsprocessen in lijn met de organisatiedoelstelling, standaarden en richtlijnen op het gebied van privacy. De proceseigenaren (afdelingshoofden) informeren de PO elk triaal over de staat van privacy binnen hun proces.

Alvorens aangevangen wordt met een nieuwe of verdere verwerking van persoonsgegevens wint de hoofd/proceseigenaar advies in bij de privacy officer.

7.1.8 Privacy officer
De privacy officer is vanuit de tweede lijn verantwoordelijk voor het formuleren van de strategische richting van privacybescherming in overeenstemming met organisatorische veranderingen, privacywetgeving en dreigingen. Dit gaat om het opzetten, onderhouden en uitvoeren van een privacybeschermingsprogramma voor het realiseren van de strategische richting. De privacy officer stelt jaarlijks een privacyplan op, zoals omschreven onder paragraaf 6.1.13 PDCA, dat onderdeel is van het Integrale Veiligheidsplan en door de directie wordt vastgesteld.

De privacy officer adviseert gevraagd en ongevraagd het management en de directie van het hoogheemraadschap bij de invulling van het privacybeleid en privacywetgeving. Het advies van de privacy officer is leidend voor de uitvoeringspraktijk. Voorgenomen afwijkingen worden ter besluitvorming door de proceseigenaar en privacy officer voorgelegd aan de directie om daar een beslissing over te nemen.

De privacy officer is niet verantwoordelijk voor de realisatie van privacybescherming door de (eerste) lijnorganisatie. De privacy officer monitort de status van privacybescherming en het voldoen aan alle relevante wet- en regelgeving met betrekking tot privacybescherming op basis van de periodieke interne controle voor de effectiviteit van beheersmaatregelen en rapporteert hierover aan het management, FG, directie en bestuur. Deze staat omvat in ieder geval hoe het lijnmanagement het privacybeleid implementeert en op welke wijze wordt voldaan aan de AVG en Wpg normenkaders, zodat de beslissers geïnformeerde besluiten kunnen nemen over de behandeling van privacyrisico's. Ook is sprake van een escalatielijn voor de CISO en PO naar de secretaris-directeur.

7.1.9 Functionaris Gegevensbescherming (FG)
Het hoogheemraadschap is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. Het hoogheemraadschap is daarom verplicht een FG aan te stellen en heeft dat ook gedaan. De FG is de onafhankelijke interne toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG brengt jaarlijks een verslag uit aan het College van D&H van zijn of haar werkzaamheden, bevindingen en aanbevelingen. Deze heeft betrekking op verwerkingen op grond van de AVG en de Wpg.

7.1.10 CISO
De Chief Information Security Officer (CISO) is strategisch adviseur voor het bestuur, directie en management op het gebied van informatieveiligheid en boegbeeld voor informatieveiligheid (IT en OT)[2] binnen en buiten de organisatie. De CISO formuleert de strategische richting van informatieveiligheid in overeenstemming met organisatorische veranderingen, relevante wet- en regelgeving, opkomende dreigingen en risicobereidheid van de organisatie. Daarnaast draagt de CISO zorg voor het opzetten, onderhouden en uitvoeren van een informatieveiligheidsprogramma voor het realiseren van de strategische richting. Ook stelt de CISO het strategisch Informatieveiligheidsbeleid HHNK 2025-2027 op en adviseert hierover aan het hoogheemraadschap. Tevens organiseert en stuurt de CISO de informatiebeveiliging overeenkomstig de behoeften en risicobereidheid van de organisatie. Daarbij ondersteunt hij of zij vanuit een onafhankelijke positie de organisatie bij het realiseren van een passend niveau van informatieveiligheid.

Ook draagt de CISO hierbij zorg voor een vertaling van de informatieveiligheidsdoelstellingen naar een informatieveiligheidsstrategie, -beleid en uitgangspunten. Dit omvat ook het gevraagd en ongevraagd adviseren van en rapporteren aan management, directie en bestuur over de staat van informatieveiligheid binnen het hoogheemraadschap, relevante in- en externe ontwikkelingen en risico's. Ook is sprake van een escalatielijn voor de CISO en PO naar de secretaris-directeur.

7.1.11 Interne (IT-)auditor
Onafhankelijke toetsing en rapportage over het voldoen aan het wettelijke normenkader voor de Wpg, waaronder controle op de taken van de FG daarin.

De interne (IT-)auditor voert waar nodig gerichte, onafhankelijke controle uit op naleving van (delen uit) de AVG en de bescherming van persoonsgegevens op basis van risico analyses, afstemming met de FG en/of toekomstige wettelijke ontwikkelingen.

7.1.12 Iedere werknemer
Iedereen werkzaam binnen het hoogheemraadschap is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. Het hoogheemraadschap verlangt van al haar medewerkers en alle personen die werkzaam zijn voor het hoogheemraadschap dat de voorschriften van dit privacybeleid worden opgevolgd en actief worden uitgedragen.

Voor posities binnen HHNK waarbij toegang tot zeer vertrouwelijke informatie vereist is, wordt bij de selectie van kandidaten een verificatie uitgevoerd, zoals van referenties, of een screening indien noodzakelijk. De verantwoordelijkheid met betrekking tot het bepalen van de noodzakelijkheid ligt bij het afdelingshoofd HRVCF.

Een medewerker is verantwoordelijk voor het ontwikkelen van voor de functie benodigde kennis op het gebied van privacybescherming en informatieveiligheid. Hierbij wordt onder andere gebruik gemaakt van de interventies die door HHNK worden aangeboden (bijvoorbeeld via de HHNK Academie).

Iedere medewerker is persoonlijk verantwoordelijk voor de wijze waarop deze omgaat met persoonsgegevens en overige bedrijfsmiddelen. Ook is iedere medewerker verplicht om (potentiële) datalekken en/of inbreuken op het gebied van informatieveiligheid zo spoedig mogelijk te melden bij de tweedelijns privacy organisatie via de daarvoor beschikbaar gestelde tegel in Topdesk. Daarnaast wint iedere medewerker advies in bij de privacy officer alvorens aangevangen wordt met een nieuwe of verdere verwerking van persoonsgegevens.

7.1.13 Ondernemingsraad
De Wet op de Ondernemingsraden benoemt een aantal plichten voor de ondernemer van een organisatie om voordat een definitief besluit (tot vaststelling, wijziging of intrekking) is genomen instemming te vragen bij de ondernemingsraad (hierna: OR) van die organisatie. Waar het gaat om verwerking van personeelsgegevens, heeft de OR instemmingsrecht bij:

- een regeling omtrent het verwerken van alsmede de bescherming van de persoonsgegevens van de in de onderneming werkzame personen. [3]

2) *IT staat voor informatietechnologie; OT staat voor operationale technologie*

3) *Zie artikel 27, eerste lid, onder k WOR*

- een regeling inzake voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen. [4]

Bij de uitvoering van een DPIA die de verwerking van personeelsgegevens betreft wordt door de proceseigenaar de mening van de OR gevraagd. [5]

8 Beheer en Onderhoud

De actualiteit en kwaliteit van het privacybeleid en uitwerkingen daarvan worden iedere drie jaar geëvalueerd. Veranderde wet- en regelgeving en doelstellingen van het hoogheemraadschap vormen hier een onderdeel van. Indien daartoe aanleiding bestaat wordt het privacybeleid geactualiseerd. Dit proces maakt onderdeel uit van een PDCA-cyclus.

9 Klachten

Als het hoogheemraadschap een wettelijke verplichting niet nakomt kan de betrokkene een klacht indienen. Deze zal op grond van de regels van de klachtenverordening van het hoogheemraadschap worden behandeld.

10 Inwerkingtreding en citeertitel

Dit besluit treedt in werking op de eerste dag volgende op die van haar bekendmaking.
Het 'Privacybeleid HHNK 2018', registratienummer 18.139446, wordt ingetrokken.
Dit besluit kan worden aangehaald als 'Privacybeleid HHNK 2025-2027'.

11. Responsible, Accountable, Supportive, Consulted, Informed (RASCI)

TAKEN	Responsible	Accountable	Supporting	Consulted	Informed
Algemeen					
Organisatiedoelstellingen	D&H	CHI	AH, PO	-	-
Jaarrekening	D&H	CHI	-	PO	-
Budget informatieveiligheid (waaronder privacy)	D&H	CHI	AH HRVCF PO	-	-
Hoogste ambtelijke eindverantwoordelijke op het gebied van privacy *Uitoefenen van bevoegdheden van het DB, inzake de bescherming van persoonsgegevens, voor zover deze in mandaat zijn gegeven*	Secretaris-directeur	-	Ambtelijke organisatie	-	-
Aan- en bijsturing van de eerste en tweede lijn op het gebied van privacy	Directeur Bedrijfsvoering	-	-	-	-
Aan- en bijsturing van de eerste lijn op het gebied van privacy	Directeur Water	-	-	-	-
Beleid					
Er is algemeen privacybeleid	D&H	CHI	AH HRVCF PO	FG CISO MB DO	CHI
Er zijn uitwerkingen van het algemeen privacybeleid	AH HRVCF	D&H	PO	FG CISO MB DO	-
Verantwoordelijkheden op het niveau van het lijnmanagement zijn benoemd, belegd en vastgelegd	AH HRVCF	D&H	PO	FG CISO MB DO	-
Evaluatie privacybeleid	AH HRVCF	DO	PO	FG CISO	MB

4) *Zie artikel 27, eerste lid, onder I WOR*
5) *Zie artikel 35, negende lid AVG*

Processen					
Beschrijving administratieve organisatie (procedures, AH stelt vast)	AH	DO	PO	-	-
Verwerkingsregister	AH	DO	PO	-	-
Pré-DPIA	AH	DO	PO	FG	-
DPIA	AH	DO	PO, ISO, SA	FG	-
Bewaar- en vernietigingsbeleid	AH	DO	PO	FG	MB
Organisatorische inbedding					
Privacyorganisatie	AH HRVCF	DO	PO	-	-
Privacy PDCA-cyclus	AH HRVCF	DO	PO	-	-
Privacyjaarplan	AH	DO	PO	FG	MB
Privacystandaarden (AH HRVCF stelt vast)	AH HRVCF	DO	PO	FG	MB
Privacyrichtlijnen (PO stelt vast)	AH HRVCF	DO	PO	FG	MB
Gedragsregels (directie stelt vast)	AH HRVCF	DO	PO	FG, veiligheidsmedewerkers *(fy-siek en sociaal)*	MB
Jaarverslag Privacy	AH HRVCF	DO	PO	-	FG CISO MB D&H
Aanstelling FG	AH CC	DO	AH CC	-	-
Privacybewustzijn	AH	DO	Academie	FG PO	-
Crisisbeheersing privacy	Crisisorganisatie	AH CCB	-	FG PO	-
Rechten van betrokkenen					
Verzoeken van betrokkenen	AH	D&H	PO	-	-
Samenwerking					
Er is inzicht in welke AVG-rol externe partijen innemen en er worden afspraken gemaakt conform de AVG	AH	DO	PO	-	-
Eenmalige gegevensverstrekkingen worden getoetst aan relevante privacy-wet- en regelgeving	AH	DO	PO	-	-
Gegevensbescherming					
Risicobeheersing	AH	DO	PO, SA, R&CO	FG CISO	D&H
Gegevensbescherming door ontwerp (privacy by design)	AH	DO	PO	FG	-
Gegevensbescherming door standaard instellingen (privacy by default)	AH	DO	PO	FG	-
Informatieveiligheid	AH	DO	ISO, SA	CISO	D&H
Privacy incidentbeheersing	AH	DO	Medewerkers PO	FG	DO D&H
Verantwoording					
Triaalrapportage privacyjaarplan	AH HRVCF	DO	PO	MB	FG
Triaalrapportage staat privacy	AH HRVCF	D&H	PO	MB DO	FG D&H
Triaalrapportage privacy (bij jaarrekening)	AH HRVCF	D&H	PO	MB DO	FG D&H

Toelichting RASCI
Responsible: De functionaris die **direct verantwoordelijk** is voor de juiste en tijdige uitvoering van de taak of degene die de activiteit zelf uitvoert. Hiervoor wordt verantwoording afgelegd aan de persoon die accountable is.

Accountable: De functionaris die **eindverantwoordelijk** (bevoegd) is voor de juiste uitvoering van de taak en goedkeuring geeft aan het eindresultaat. Als het erom gaat, moet deze persoon het eindoordeel kunnen vellen, vetorecht hebben. Deze functionaris is geheel afhankelijk van het succes waarmee R de activiteit uitvoert. Vooral ook omdat A vaak voor het totaal van het proces eindverantwoordelijk is, als proceseigenaar. In veel gevallen is A iemand hoger in de hiërarchie dan R, maar dat hoeft niet per se.

Supporting: De functionaris die **ondersteuning** verleent aan de uitvoering van de taak of de taak uitvoert. S is een ondersteunende rol waarop R een beroep kan doen. Kan alleen op verzoek van R support leveren. Deze persoon is een expert op zijn gebied. S is verantwoordelijk voor de kwaliteit en het resultaat van zijn support maar is niet direct verantwoordelijk voor de activiteit zelf.

Consultable: De functionaris die **vooraf** geraadpleegd moet worden of goedkeuring of input moet leveren bij een activiteit in het proces. Deze persoon kan daarmee dus het resultaat nog beïnvloeden.

Informed: De functionaris die **achteraf** geïnformeerd moet worden over de beslissingen, over de voortgang of bereikte resultaten. Deze persoon kan het resultaat dus niet meer beïnvloeden.