



Hoogheemraadschap van
Rijnland

FG jaarverslag 2023 Rijnland

Document:	FG jaarverslag 2023
Versie:	1.0
Auteurs:	Bianca Steentjes (Functionaris Gegevensbescherming)
Datum vaststelling DT:	25 januari 2024
Corsa registratienr:	24.008854

Aanleiding

Jaarlijks geeft de Functionaris Gegevensbescherming (hierna FG) inzicht in de stand van zaken met betrekking tot Privacy en het naleven van de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) bij het Hoogheemraadschap van Rijnland (HHR).

Dit jaarverslag wordt voorgelegd aan het DT van HHR, waarbij gevraagd wordt te besluiten over de aanbevelingen. Omdat formeel het dagelijks bestuur de eindverantwoordelijke is, gaat dit jaarverslag na bespreking met de directie naar de portefeuillehouder Privacy en wordt daarna ter kennisgeving voorgelegd aan D&H en het algemeen bestuur.

Het jaarverslag 2023 is tot stand gekomen op basis van documenten van de vertrokken FG (Linda van Mourik) van HHR, informatie van de vorige FG van HHSK (Doreen Wilbers) en de nieuwe FG (Bianca Steentjes).

De aanbevelingen zijn gebaseerd op de onderzoeken uitgevoerd in de eerste helft van 2023 in combinatie met de bevindingen van de nieuwe FG. Omdat geen informatie voor handen was over de bevindingen van de vorige FG ten aanzien van haar rol voor de Rekenkamercommissie is hierover geen informatie opgenomen.

Privacy wet- en regelgeving

In 2018 is de AVG van kracht geworden en heeft privacy haar plek gekregen binnen organisaties in Nederland, zo ook binnen HHR. Op basis van de AVG is HHR verantwoordelijk voor de borging van de privacy in de omgang met inwoners en personeel. Daarnaast heeft HHR vanuit de AVG een 'verantwoordingsplicht'. HHR moet met documenten kunnen aantonen dat het de juiste organisatorische en technische maatregelen heeft genomen om aan de AVG wet- en regelgeving te voldoen.

De laatste jaren is sprake van veel ontwikkelingen op digitaal gebied. De EU ziet de digitale transitie als essentieel voor de economische ontwikkeling en strategische autonomie van de EU is. Hiervoor is de 'Digitale Strategie' opgesteld, die leidt tot veel privacy gerelateerde EU-wetgeving. Voor de waterschappen zijn in 2023 geen (aanvullende) privacy gerelateerde EU wetten van toepassing geworden. In 2024 zal de NIS2¹ en mogelijk de AI Act in werking treden.

In 2023 zijn wel nieuwe afspraken gemaakt ten aanzien van gegevensuitwisseling buiten de EER. De waterschappen hebben via het programma IB&P van het Waterschapshuis de verwerkersovereenkomst hierop aangepast.

Vanuit de Autoriteit Persoonsgegevens (AP) wordt onafhankelijk toezicht gehouden op de naleving van de AVG. Jaarlijks benoemt de AP een aantal aandachtspunten waar zij aandacht aan geven. Voor 2023 heeft zij zich gefocust op: datahandel, digitale overheid en AI en Algoritmes.

¹ NIS2: De Network and Information Security directive is de opvolger van de NIS-richtlijn en bedoeld om de cyberbeveiliging en weerbaarheid van essentiële diensten in EU-lidstaten te verbeteren. NIS2 gaat ook gelden voor overheden.

Kernteam privacy en de FG

Kernteam privacy

Sinds medio 2022 heeft HHR alle functies behorende bij een volwassen uitvoering van de AVG ingevuld. In 2023 is aandacht besteedt aan het beleggen van de bijhorende taken tussen de FG en het kernteam privacy. Het kernteam privacy bestaat uit de privacy officer, twee juristen en een communicatiespecialist. Het team heeft grote stappen gezet in de groei van volwassenheid van de inrichting en deels de werking van privacy in de organisatie.

Doordat de privacy officer voor 0,5 fte gedetacheerd is vanuit HHSK wordt de samenwerking tussen beiden organisaties bevorderd en wordt meer efficiëntie behaald.

De privacy officer ondersteunt met de kernteam privacy de eerste lijn (teamleiders en privacy contactpersonen) door het beantwoorden van vragen, het behandelen van incidenten en datalekmeldingen en het opzetten en monitoren van kaders zoals beleid en protocollen. Veel tijd wordt besteed aan de organisatiebrede bewustwording op het gebied van privacy en informatiebeveiliging. Tevens zijn in 2023 verdere stappen gezet om de PDCA-cyclus meer vorm te geven. In het derde kwartaal hebben de kernteam privacy en de FG de focus gelegd op uitvoering van tweede audit op de AVG/BIO en de reactie op de conceptrapportage van de externe auditor.

Functionaris Gegevensbescherming

Tot 7 september 2023 was Linda van Mourik voor ca. 0,6 fte aangesteld als FG. Zij werkte nauw samen met de FG van HHSK en het landelijk forum van FG's bij waterschappen. Per 1 oktober is de functie van FG overgenomen door Bianca Steentjes. Zij is voor 0,4 fte gedetacheerd naar HHSK, waar zij dezelfde functie uitvoert. Hierdoor zal veel informatie gedeeld kunnen worden met/tussen de Hoogheemraadschappen. Bianca zal ook aansluiten bij de overleggen met de privacy officers en de FG's van de waterschappen.

De FG adviseert de organisatie over Privacy onderwerpen die zich daarvoor aandienen. Daarnaast heeft de FG Data Protection Impact Assessments (DPIA) beoordeeld en geadviseerd over het al dan niet uitvoeren van DPIA's, zijn verslagen goedgekeurd en indien van toepassing worden datalekken gemeld bij de AP. Tevens is steekproefsgewijs toezicht gehouden op de AVG-compliance van de teams en is aan directie gerapporteerd en geadviseerd.

Informatieveiligheid en Privacy hebben veel punten van overlap. De samenwerking op het gebied van Privacy en Informatieveiligheid tussen de hoogheemraadschappen bevordert de kennisuitwisseling. Bovendien leidt de samenwerking tot verbetering en eenduidigheid in alle twee de organisaties. Door de samenwerking op het gebied van de salarisadministratie en financiën sluiten de privacy officer en FG van het Hoogheemraadschap van Delfland (HHD) vaker aan.

Via de waterschapsbrede FGW (FG's van waterschappen) worden gezamenlijke onderwerpen uitgewerkt en afgestemd.



**Externe audits
BIO/AVG + Wpg**



DPIA's

1. Corsa in de cloud + connector
2. Centrale salarisadministratie (HHR, HHSK en HHD)



**FG-onderzoeken
i.s.m. FG's HHSK
en HHD**



**Datalek gemeld
bij AP**



**Kwartaalgesprekken
CISO/PO/FG/SAD/
Directeur BV**



**Week van de
Privacy 5-jarig
bestaan AVG en
interne opleiding**

Resultaten (externe) onderzoeken

BIO/AVG audit 2023

Eind 2023 heeft bureau Verdonk, Klooster & Associates (VKA) de uitkomsten van het door haar in september 2023 uitgevoerde onderzoek bij HHR opgeleverd. Het onderzoek binnen HHR is onderdeel van de sectorbrede audit aanbesteed door het programma IB&P van het Waterschapshuis namens alle waterschappen. Op het moment van het opstellen van dit jaarverslag was het sectorgemiddelde nog niet gepubliceerd.

VKA geeft in haar management samenvatting aan dat HHR sinds de eerder uitgevoerde audit (2021), duidelijk aandacht heeft besteed aan het verbeteren van haar kantoor- en procesautomatisering en het verantwoord omgaan met privacygevoelige gegevens. Het uitvoeren van de geïmplementeerde informatieveiligheid en privacy maatregelen vindt plaats op organisatie- en afdelingsniveau onder verantwoordelijkheid van het lijnmanagement.

Voor het onderdeel privacy zijn, door VKA, de volgende scores bepaald:

- Het managementsysteem voor privacy scoort qua volwassenheid **2,9**. Dit is een duidelijke verbetering ten opzichte van de 2,2 in 2021.
- Het Hoogheemraadschap scoort met **3,8** bijna conform de gewenste volwassenheid, voor het verantwoord omgaan met privacygevoelige gegevens. Dit is een grote verbetering ten opzichte van de 3,0 in 2021.

De nieuwe FG stelt vraagtekens bij de bevindingen die VKA heeft gedaan ten aanzien van de werking² van maatregelen. De werking is enkel getest door vragen te stellen gedurende de interviews en het beoordelen van ingezonden documenten en niet door een systeem te testen.

In de rapportage zijn door VKA maatregelen beschreven om de noodzakelijke verbeteringen door te voeren. Bij de verbeteringen is het uitgangspunt om een score van 4,0 te realiseren. Het kernteam privacy zal in overleg met de FG, gezamenlijk met de proceseigenaren, bepalen welke maatregelen nodig zijn om de gewenste resultaten voor HHR te behalen, rekening houdend met de wensen van de directie en het bestuur.

Onderzoeken FG 2023

De onderzoeken zijn uitgevoerd door de vorige FG's van HHR en HHSK. De onderstaande samenvatting is voortgekomen uit de ontvangen rapportages.

- A) Een onderzoek is uitgevoerd naar de aanbesteding securitydiensten (in 5 percelen) bij HHR en HHSK. Het onderzoek is uitgevoerd in samenwerking met de vorige FG van HHSK (Doreen Wilbers).

Het onderzoek van de FG's heeft zich gericht op de aanbesteding van perceel 5 – Awareness, met name phishing campagnes, gegund aan Secura. Deze is aanbesteed zonder de privacydeskundigen daarbij te betrekken, terwijl juist Awareness een grote overlap heeft tussen informatieveiligheid en Privacy. De aanbesteding is vooralsnog daardoor alleen gericht op informatieveiligheid.

Voor 2 van de 5 percelen zijn de verwerkingen nog niet in het verwerkingsregister gezet. De betrokkenheid van de OR en over de noodzaak van het uitvoeren van een DPIA staan nog vragen open. Uit het onderzoek is verder naar voren gekomen dat de afdeling Inkoop behoefte heeft aan een nadere toelichting en hulp bij gebruik van de ICO-tool voor o.a. privacy.

² Wordt gewerkt op de manier zoals we dit hebben beschreven.

- B) De FG heeft een oordeel gegeven met betrekking tot de Data Protection Impact Assessment (DPIA) voor het proces van de gezamenlijke/ Centrale Salarisadministratie en het Functioneel beheer daarvan voor het HHR, HHSK en het Hoogheemraadschap van Delfland (HHD).

Gevraagd is een oordeel te geven ten aanzien van het voldoen van de persoonsgegevensverwerkingen aan de eisen van de AVG. Dit houdt in een oordeel over de geconstateerde privacyrisico's in de persoonsgegevensverwerkingen en de voorgestelde maatregelen daarop.

Per geconstateerd risico is door de FG's een oordeel gegeven. Op 22 mei 2023 is door de Stuurgroep besloten tot livegang van de gezamenlijk gevoerde salarisadministratie op 1 juli 2023. Met dit besluit en het opleveren van de DPIA door het project was het niet mogelijk om vóór de livegang een aantal maatregelen om privacyrisico's te mitigeren te implementeren. Deze termijn is daarom verlengd met 3 maanden na livegang.

De belangrijkste prioriteiten met hoog risico zijn:

- Testen met kopie van de productiedata is een verwerking voor een ander doel en hiermee onrechtmatig.
- Het risico bestaat dat de integriteit van de data in het geding is.
- Uitwisseling van gegevens en controlechecklists tussen de Salaris- en Personeelsadministratie gaat buiten eHRM om (via mail en O365). Dit is kwetsbaar en onbeveiligd. Verkenning van gebruik van gezamenlijke sharepoint is hoogstwaarschijnlijk niet voor de livegang afgerond.
- Bij in-, door- en uitstroom is niet geborgd dat automatisch de verleende toegang tot de systemen ook wordt gewijzigd of geblokkeerd, met als risico onrechtmatige toegang.

Verder is aan het voldoen aan de (aantoonbare) verwijdering van persoonsgegevens na verlopen van de bewaartermijnen een hogere urgentie toegekend. Het nieuwe e-HRM systeem zal ingericht moeten worden op het hanteren van de juiste bewaartermijnen en verwijdering van gegevens na verloop daarvan.

Voorstel was om eind oktober 2023 een nieuwe FG-toets te doen. Deze toets is door vertrek van de drie FG's niet uitgevoerd. Eind 2023 zijn de privacy officers van de drie waterschappen samen met de nieuwe FG gestart met het in kaart brengen van de nodige acties rekening houdend met de laatste ontwikkelingen.

- C) Een onderzoek is uitgevoerd naar de aanbesteding van het wagenpark. Het onderzoek is uitgevoerd in samenwerking met de vorige FG van HHSK (Doreen Wilbers).

De lease van het wagenpark van HHSK is aanbesteed. Het ging om een meervoudig onderhandse aanbesteding. In de concept Overeenkomst is gegevensverwerking meegenomen bij het in de markt zetten van de uitvraag. Onduidelijk is of deze verwerkersovereenkomst nu ook is opgenomen in het verwerkersregister. Eveneens is onduidelijkheid of een DPIA is opgesteld en in welke fase van de aanbesteding dit heeft plaatsgevonden*.

*Voor HHR is de DPIA voor het wagenpark uitgevoerd. Op 4 april 2022 is gerapporteerd aan de teamleider Facilitaire Zaken. De genoemde risico's zijn tot op heden nog niet gemitigeerd.

Audit Wet politiegegevens (Wpg) 2023 – 0-meting

In 2023 heeft BakerTilly een externe audit uitgevoerd op de naleving van de Wpg. De Wpg heeft betrekking op gegevensverwerking in het kader van (strafrechtelijke) opsporing. Alle organisaties die

Boa-werkgever zijn, zijn sinds 2019 verplicht om een reguliere externe audit op de Wpg te laten uitvoeren en het rapport te delen met de AP.

Deze audit was de eerste audit op de naleving van de Wpg en ziet de organisatie, maar ook de externe auditor, als een 0-meting. De audit had betrekking op de periode 2021 en is uitgevoerd in 2023.

In december 2023 heeft de auditor het conceptrapport met HHSK gedeeld. De auditor concludeert daarin dat: "Naar ons oordeel, in alle van materieel belang zijnde aspecten, zijn de door Hoogheemraadschap van Rijnland getroffen beheersingsmaatregelen om te voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's niet gedurende de gehele verslagperiode van 9 maart 2019 t/m 31 december 2021, respectievelijk de 12 maanden voorafgaand aan de einddatum van de externe privacy audit Wpg 2021 in afdoende mate opgezet, hebben niet bestaan en/of werkten niet effectief." Dit heeft geleid tot een afkeurend oordeel. In januari 2024 zal de BakerTilly een presentatie geven in het CPW-overleg.

Vanaf 1 oktober 2023 voldoet HHSK aan de wettelijke verplichting om voor de Wpg een FG aan te stellen.

Bewustwording organisatie

Bij HHR heeft in de week van 25 mei 2023 een organisatiebrede "Week van de Privacy", in verband met het 5-jarige bestaan AVG, plaatsgevonden. Hierbij zijn veel activiteiten georganiseerd in het kader van de bewustwording met focus op datalekken, zoals escape-rooms, pub-quizen en een interne opleiding. Verder stond het kernteam privacy de hele week in de centrale hal om met medewerkers, directie- en bestuursleden in discussie te gaan over privacygerelateerde onderwerpen en om vragen te beantwoorden. Het kernteam privacy heeft in die week ook enkele buitenlocaties bezocht om ook de bewustwording daar niet te vergeten. Deze persoonlijke aandacht werd door de buitendienstmedewerkers zeer op prijs gesteld.

Inzage, informatieverzoeken en datalekken

Inzage en informatieverzoeken

In 2023 zijn bij HHR twee inzage- of informatieverzoeken van burgers op grond van de AVG binnengekomen. Het eerste verzoek is door de verzoeker ingetrokken. Het tweede verzoek is buiten behandeling gelaten, nadat de verzoeker niet heeft gereageerd op een verzoek tot identificatie op kantoor.

In 2023 was tevens sprake van een inzageverzoek, die landelijk was ingediend bij alle waterschappen en voor de uiterlijke beslistermijn weer ingetrokken. De aanleiding van dit inzageverzoek was een juridisch conflict tussen deze verzoekende partij en het Waterschapshuis.

Datalekken

HHR heeft een meldplicht voor datalekken, waardoor HHR direct een melding moeten doen bij de AP, zodra sprake is van een ernstig datalek. In bepaalde gevallen moet het datalek ook gemeld worden aan de betrokkenen. De AVG vereist tevens dat alle datalekken binnen een organisatie gedocumenteerd worden. Met deze documentatie moet de AP kunnen controleren of organisaties aan de meldplicht datalekken hebben voldaan.

In 2023 is vlak voor de feestdagen één voorlopige datalek melding gedaan bij de AP in afwachting van verder onderzoek naar een incident van diefstal van laptops. De overige datalekken bleven intern (er zijn 18 privacy meldingen in Topdesk geregistreerd). Deze hadden naar het oordeel van de privacydesk en de FG geen zodanige impact voor burgers/medewerkers dat een melding bij de AP of bij de betrokkene nodig was.

De meeste incidentmeldingen betroffen nog steeds verkeerd verstuurde mails of verkeerde/onbeveiligde gevoelige bijlagen.

Verwerkingsregister en verwerkingsovereenkomsten

HHR is vanuit de AVG verplicht om een verwerkingsregister bij te houden waardoor zichtbaar is welke verwerkingen van persoonsgegevens worden uitgevoerd. Tijdens de externe audit door VKA is het verwerkingsregister op basis van de CIP Privacy Volwassenheidsmodel getoetst en geconstateerd dat HHR zicht heeft op de verwerkingen aan de hand van de verwerkingsregister en het register periodiek wordt bijgehouden.

Als HHR bij de verwerking een derde partij inschakelt, dan worden de verantwoordelijkheden geregeld in een verwerkingsovereenkomst. In de verwerkingsovereenkomst zijn afspraken omtrent de belangrijkste beginselen van een verwerking, zoals rechtmatigheid, transparantie, doelbinding en juistheid, opgenomen. HHR maakt gebruik van de verwerkingsovereenkomst zoals opgesteld door het Waterschapshuis.

Overlegstructuren

Interne overleggen

Het kernteam privacy overlegt 4-wekelijks, waarbij de FG uitgenodigd is om deel te nemen aan het overleg. De nieuwe FG zal dit in eerste instantie structureel doen om inzicht te krijgen in de privacy vraagstukken binnen HHR. Daarnaast vindt eens per kwartaal een overleg plaats tussen het kernteam privacy en de privacy contactpersonen binnen HHR. In 2023 hebben de contactpersonen op relevante thema's een verdiepende training gehad, bijvoorbeeld over datalekken of verwerkersovereenkomsten. Hiermee kunnen zij beter in hun rol zitten als eerstelijns vraagbaak.

CPW en FGW

De FG's en privacy officers werken landelijk samen in het Contactpersonenoverleg Privacy Waterschappen (CPW) dat is ondergebracht in het programma Informatieveiligheid en privacy van Het Waterschapshuis. Het CPW is voor vragen en maatregelen die sectorbreed moeten worden opgepakt. Daarnaast komen de FG's van de waterschappen geregeld bijeen in het Landelijke Overleg voor FG's van de waterschappen (FGW).

De privacy officer en privacy juristen leveren een actieve bijdrage aan het CPW, bijvoorbeeld door deelname aan werkgroepen ter verbetering en aanpassing van de model verwerkersovereenkomst.

Conclusie

De vorige FG's hebben gezamenlijk een mooie basis gelegd met de eerste FG-toezichtactiviteiten, maar er is op het gebied van PDCA nog wat werk te doen. Dit is ook wel gebleken uit de VKA-audit. Goed om te zien dat dit een prominente plek krijgt in het jaarplan 2024 van het kernteam privacy.

In samenwerking met de privacy officer zal de FG haar functie in 2024 verder vorm gaan geven. Gestart is met het opstellen van een auditplan 2024 aansluitend bij het jaarplan 2024 van het kernteam privacy. De FG wordt op de hoogte gehouden van de voortgang en uitwerking van het jaarplan 2024 en gevraagd of ongevraagd advies geven. Andersom zal de FG de privacy officer meenemen in haar bevindingen.

Met betrekking tot de Wpg is sprake van een situatie waarin bij het opstellen van het verbeterplan goed gekeken moet worden welke stappen/ maatregelen als eerste genomen moeten worden gezien het te lopen risico en de tijdsbesteding van de medewerkers. Voor de Wpg ligt de toezichthoudende taak bij de FG, echter er is geen team in de tweede lijn die adviseert.