RAADSINFORMATIEBRIEF

VAN HET COLLEGE VAN B&W
VOOR de gemeenteraad
CC
DATUM 4 maart 2025
ONDERWERP Jaarverslag Functionaris Gegevensbescherming 2024

Geachte gemeenteraad,

In deze raadsinformatiebrief informeren wij uw gemeenteraad over het Jaarverslag van de Functionaris Gegevensbescherming 2024.

Onderstaand de samenvatting met daarin de belangrijkste uitkomsten van het verslag en daarnaast in de bijlage het volledige verslag. Wij hopen u hiermee voldoende geïnformeerd te hebben.

Het verslag is opgesteld door de Functionaris Gegevensbescherming (FG) die sinds januari 2024 deze rol bekleedt. De FG ziet als onafhankelijke interne toezichthouder toe op naleving van Algemene verordening gegevensbescherming (AVG) en Wet Politiegegevens (Wpg).

De conclusie van het jaarverslag is dat de Algemene Verordening Gegevensbescherming (AVG) en de Wet Politiegegevens (WPG) op een juiste wijze binnen de gemeente Krimpenerwaard wordt toegepast.

De FG doet 5 aanbevelingen in zijn jaarverslag om de toepassing verder te verbeteren.

- Implementeer het werkproces datalekken zodat de stijgende lijn uit 2024 vast gehouden kan worden
- Geef uitvoering aan het voornemen om de AVG-procedure “inzage persoonsgegevens en de inzageverzoeken uit andere wetgeving” voor de burger duidelijker te organiseren
- Vergroot de kennis en ervaring op het gebied van Artificiële Intelligentie (AI geletterdheid)
- Geef uitvoering aan het opstellen van een verbeterplan voor de punten uit de WPG-audit
- Maak nadat de pilot is afgerond een plan voor de uitvoering van de “must have DPIA’s” van de VNG.

Deze aanbevelingen zijn door de Privacy Officer (PO) en de teammanager Concern Control waar de PO onderdeel van is herkend en worden opgepakt.

Bijlage: Jaarverslag FG 2024

Met vriendelijke groet,
burgemeester en wethouders van Krimpenerwaard,

de secretaris, de burgemeester,

J. Hennip ir. J. Beenakker

gemeente Krimpenerwaard

Jaarverslag 2024

Functionaris Gegevensbescherming

Algemene Verordening Gegevensbescherming

Wet Politiegegevens

Datum: 5 februari 2025

Functionaris: [redacted]

1. Inhoudsopgave

2. Managementsamenvatting

Het algemene beeld is dat de bescherming van persoonsgegevens binnen de Gemeente Krimpenerwaard voldoende is. Medewerkers en directie/management zijn zich bewust van de persoonsgegevens waar ze mee om gaan en de vereisten die dat met zich meebrengt. Er is voldoende bewustzijn en waar nodig wordt de kennis verder verbeterd. De organisatie staat er ook voor open om zich op dit gebied te ontwikkelen.

In 2024 is door het College van Burgemeester & Wethouders het vernieuwde privacy beleid vastgesteld. De vaststelling is een katalysator voor het verantwoord om gaan met persoonsgegevens.

De volgende stap is dat dit beleid wordt geïmplementeerd in de bestaande werkprocessen. Dat geldt ook voor de privacy processen “melding van een datalek” en “uitvoeren van een DPIA”, die in het vorige jaarverslag als aandachtspunten werden genoemd. Deze zijn reeds uitgewerkt en zullen in 2025 geïmplementeerd worden.

De vereiste AVG documentatie die nodig is om de inspanningen aantoonbaar te maken, is aanwezig, zij het dat dit voor een deel nog “work in progress” is (Register van Verwerkingsactiviteiten).

Voor de stand van zaken met betrekking tot de implementatie van de Wpg en Bpgboa heeft een extern bureau aan het begin van het jaar een audit gehouden. Uit deze audit kwamen een aantal verbeterpunten naar voren. In 2025 zal hiervoor een verbeterplan worden opgesteld.

Aanbevelingen

Op basis van het verslag doe ik als FG de volgende aanbevelingen:

- Implementeer het werkproces datalekken zodat de stijgende lijn uit 2024 vast gehouden kan worden;
- Geef uitvoering aan het voornemen om de AVG-procedure “inzage persoonsgegevens en de inzageverzoeken uit andere wetgeving voor de burger” duidelijker te organiseren;
- Vergroot de kennis en ervaring op het gebied van Artificiële Intelligentie (AI geletterdheid);
- Geef uitvoering aan het opstellen van een verbeterplan voor de punten uit de WPG-audit;
- Maak nadat de pilot is afgerond een plan voor de uitvoering van de “must have DPIA’s” van de VNG.

3. Deel A AVG

3.1 Terugblik 2024

3.1.1 Beleid

In 2024 is het privacy beleid dat dateerde uit 2018, het jaar van de invoering van de AVG, door de Privacy Officer geüpdatet. Sinds de invoering van de AVG zijn de inzichten vernieuwd en heeft de aanpak van privacy vraagstukken zich verder ontwikkeld. Een update was daarom noodzakelijk. Het beleid beschrijft hoe de Gemeente Krimpenerwaard om gaat met de persoonsgegevens die zij verwerkt. Naast de principes en uitgangspunten die daarbij gehanteerd worden, zijn ook de rollen en verantwoordelijkheden beschreven in het Three Lines model. Dit model geeft aan wie voor welke taak met betrekking tot privacy verantwoordelijk is.

Na een review door de FG, is het beleid besproken in het Directie Team. Deze bespreking leidde tot een aantal aanpassingen, waarna de Directie het beleid heeft geaccordeerd. In het najaar is het beleid door het College van Burgemeester & Wethouders vastgesteld. Vervolgens is de Gemeenteraad geïnformeerd over het beleid.

Het vernieuwde beleid noopt ook tot het aanpassen van een aantal werkprocessen op het gebied van privacy. Dit zijn:

- Afhandelen nieuwe verwerking;
- Melding en afhandeling datalekken;
- Uitvoeren rechten betrokkenen;
- Afsluiten verwerkingsovereenkomsten;
- Uitvoeren DPIA’s.

3.1.2 Processen

Register verwerkingsactiviteiten

De Gemeente heeft er voor gekozen het Register van Verwerkingen op te nemen in de applicatie die ook de werkprocessen beschrijft. In deze applicatie zijn in 1 oogopslag het werkproces en de vereisten van de AVG te raadplegen.

De werkwijze daarvoor is als volgt. Het team Concern Control beschrijft in overleg met de proceseigenaren de werkprocessen. De Privacy Officer is hier actief bij betrokken en voegt de AVG vereisten toe. De FG beoordeelt de nieuwe verwerking en voert een pre-scan Data Protection Asessment (DPIA) uit. Deze pre scan heeft tot doel om te beoordelen of er een verplichting is om een zogenaamde DPIA uit te voeren. In de paragraaf DPIA’s wordt hier verder op in gegaan.

DPIA's

Een van de bevindingen uit het jaarverslag van de vorige FG is dat er meer aandacht moet komen voor het uitvoeren van Data Protection Impact Assessments (hierna: DPIA).

Een DPIA moet voor bepaalde verwerkingen met een hoog risico uitgevoerd worden. Het resultaat van de DPIA is dat de privacy risico's en de maatregelen om deze te mitigeren voldoende in beeld zijn. De proceseigenaar initieert op basis hiervan vervolgacties en bewaakt de restrisico's.

Om hiervoor de juiste tools aan te bieden is het proces van het uitvoeren van een DPIA beschreven, het model voor de DPIA vernieuwd en worden workshops over het uitvoeren van een DPIA gegeven. Dit alles met het doel om de DPIA laagdrempeliger te maken en daarmee het aantal uitgevoerde DPIA's te verhogen.

In 2024 is op 13 hoog risico processen een DPIA uitgevoerd waarop de FG heeft geadviseerd. In 2023 waren dit er, voor zover dit te achterhalen is, twee stuks.

Naast dat in de pre-scan DPIA geconcludeerd kan worden dat een DPIA uitgevoerd moet worden, heeft de VNG in het najaar van 2024 een lijst met zogenaamde "must have DPIA's" uitgebracht. Dit zijn verwerkingen waarvan de VNG vindt dat hiervoor een DPIA moet worden uitgevoerd. Deze lijst is besproken met het management en heeft geleid tot een pilot proces waarin het integraal uitwerken van DPIA's in 2025 en verder gestalte gaat krijgen.

Rechten betrokken

In de eerste helft van 2024 heeft 1 betrokkene (degene van wie gegevens worden gebruikt) een beroep op zijn/ haar rechten gedaan. In het onderhavige geval betrof dit het recht op inzage.

Daarbij is gebleken dat voor de verzoekers niet altijd duidelijk is, wat voor verzoek ze willen doen: een AVG verzoek, WOO verzoek of inzage uit de gegevens uit de BRP.

In het jaarplan voor 2025 van het team Concern Control is daarom opgenomen dat samen met Juridische Zaken gekeken zal worden hoe dit voor de burger duidelijker en toegankelijker kan worden gemaakt.

Datalekken

In het jaarverslag over 2023 doet de vorige FG de aanbeveling om de organisatie meer bewust te maken van incidenten waarbij mogelijk sprake is van een datalek. Om het proces te verbeteren en voor de medewerkers te vereenvoudigen, heeft de

FG een handreiking geschreven hoe dit proces ingericht kan worden. Bij het schrijven van dit verslag wordt aan de implementatie gewerkt.

In de eerste helft van 2024 zijn er 27 meldingen van een datalek geregistreerd. Ten opzichte van 2022 en 2023 is dit een forse toename (2022: 8 meldingen, 2023: 9 meldingen). Als deze trend zich in 2025 door zet kan geconcludeerd worden dat het bewustzijn van medewerkers hierover is toegenomen.

Geen van de gemelde datalekken had een dermate grote impact dat gemeld is aan de Autoriteit Persoonsgegevens.

3.1.3 Organisatorische inbedding

Voor een goede bescherming van de persoonsgegevens is het noodzakelijk dat alle medewerkers van de Gemeente bekend zijn met het belang van privacy en de beginselen van de AVG. Om dat te bewerkstelligen is de inhouse basiscursus “bescherming van persoonsgegevens” opgenomen in het onboarding programma van nieuwe medewerkers. Vanaf het voorjaar 2024 kunnen ook medewerkers die reeds in dienst zijn zich hiervoor inschrijven. In 2024 hebben rond de 80 medewerkers de cursus gevolgd.

Om deze basiscursus meer praktisch te maken zijn tevens 2 nieuwe workshops ontwikkeld en gegeven: “de AVG toegepast ”en “Hoera een DPIA”.

Daarnaast is begin van het jaar een start gemaakt met een specifieke cursus voor medewerkers in het Sociaal domein. Zij verwerken veel gegevens en doel van deze cursus, gegeven door 2 externe specialisten, was om meer praktisch en specifiek de gegevensbescherming te bespreken in dit domein.

Naast opleidingen wordt op intranet maandelijks een blog gepubliceerd over thema’s die betrekking hebben op de bescherming van persoonsgegevens.

Naast bewustzijn bij medewerkers is kennis en bewustzijn bij Directie en Management van belang. In het beleidsplan is ook de governance van de gegevensbescherming uitgewerkt: welke rollen en taken hebben Directie en Management ten aanzien van de bescherming van persoonsgegevens.

Tijdens de presentatie van het beleid in het Directieteam bleek dat de Directie zich bewust is van de noodzaak persoonsgegevens van de burgers goed te beschermen.

Nadat het beleid is vastgesteld door het College is een presentatie hierover gegeven tijdens het management overleg waar alle team managers aanwezig waren. Ook hier bleek er goede belangstelling voor het onderwerp.

Tussen de verantwoordelijke directeur en de FG vind maandelijks overleg plaats. Daarnaast hebben de teammanager/directielid Concern Control, de Privacy Officer, de CISO en de FG maandelijks overleg om actuele zaken te bespreken

3.2 Vooruitblik 2025

3.2.1 Beleid

Het jaar 2025 zal in het teken staan van de implementatie van het beleid. Dat wil zeggen dat de processen uitgewerkt worden en ter goedkeuring aangeboden worden aan de Directie en/of de daartoe bevoegde directeur. Voor het proces “rechten van betrokkenen” zal dit samen met Juridische Zaken uitgewerkt worden (zie 3.1.2).

3.2.2 Processen

Register verwerkingsactiviteiten

Het Register is nog steeds “work in progress” binnen het team Concern Control. In 2025 is het streven om de verwerkingen waarvoor de VNG lijst “must have DPIA’s geldt, in de daartoe in gebruik zijnde applicatie compleet te hebben.

DPIA’s

Als de DPIA met een van de teams is uitgevoerd is een model werkwijze voorhanden die binnen de andere teams in 2025 en de daarop volgende jaren kan worden uitgerold.

Rechten betrokken

De verwachting is in dat 2025 de verbeterde procedure in samenhang met andere verzoeken die de inwoners aan de gemeente kunnen doen vorm zal krijgen.

Datalekken

De inzet is om de in 2024 stijgende lijn van datalek meldingen voort te zetten in 2025. Een eenvoudigere datalekmelding en gericht werken aan bewustwording door korte presentaties tijdens de team overleggen moet hiervoor zorgen.

3.2.3 Organisatorische inbedding

De huidige activiteiten zoals de basiscursus, workshops en de maandelijkse blog zullen worden gecontinueerd.

Daarnaast zullen de presentaties over datalekken in alle teams verder bijdragen aan inbedding van het onderwerp in de organisatie. In overleg met het team

communicatie zal bekeken worden welke acties verder nog op gezet kunnen worden.

4. Deel B WPG

4.1.1 Terugblik 2024

In februari 2024 heeft een extern bureau een tussentijdse privacy-audit uitgevoerd op de Wet politiegegevens (WPG) en het Besluit politiegegevens voor buitengewoon opsporingsambtenaren (Bpgboa). In deze audit zijn alleen de beheersmaatregelen die in de eerdere audit “voldoet deels” of “voldoet niet” scoorden opnieuw bekeken.

De volgende adviezen worden in het auditrapport gegeven:

- Voer DPIA’s uit voor de WPG gerelateerde verwerkingen zodat voldaan wordt aan het privacy beleid.
- Documenteer de uitgangspunten van de autorisaties in een eenvoudige autorisatiematrix en controleer halfjaarlijks de autorisaties op de netwerkmap.
- Laat het BySpy rechtenbeheer ook via Topdesk verlopen.
- Controleer bij de periodieke controle op autorisaties en logging ook of onterecht Wpg-gegevens in Djuma of netwerkschrijven zijn verwerkt. Formaliseer deze controle.
- Zorg dat alle verzoeken met betrekking tot de “rechten van betrokkenen” opvraagbaar zijn, zodat snel gekeken kan worden of het verzoek is toegekend of afgewezen.
- Controleer of het nieuwe proces voor risico gebaseerde controles op de logging in de praktijk ook werkt.

In het rapport wordt geadviseerd om binnen 3 maanden na afronding van de audit een verbeterrapport op te stellen waarin de maatregelen worden beschreven die getroffen zijn om de geconstateerde tekortkomingen te verbeteren (punt 1.4). Door gebrek aan capaciteit veroorzaakt door ziektes en vacatures kon dit in 2024 niet gerealiseerd worden.

4.2 Vooruitblik 2025

Het opstellen van een verbeterrapport voor de punten uit de audit is voor 2025 opgenomen in het jaarplan. Daarmee is de uitvoering van deze actie voor 2025 geborgd.

5. Ontwikkelingen

5.1 Artificial Intelligence

Een van de belangrijkste ontwikkelingen op dit moment is onmiskenbaar de rol van Artificial Intelligence (AI). De ontwikkeling van applicaties met AI heeft een grote vlucht genomen.

De Europese AI Act die nog vertaald zal worden naar Nederlandse wetgeving beoogt een juridisch kader te geven om de ontwikkeling en het gebruik van AI te faciliteren.

De gemeente Krimpenerwaard heeft het beleid om zelf geen AI toepassingen te ontwikkelen. Dat betekent echter niet dat de gemeente niets van doen heeft met AI.

Allereerst is niet uit te sluiten dat medewerkers zelf al AI toepassingen zoals ChatGPT gebruiken om hen te ondersteunen bij hun werk.

Ten tweede gebruiken veel leveranciers van applicaties AI in hun toepassingen. Als de Gemeente applicaties met AI gebruikt, zal zij ook aan de AI Act moeten voldoen. De AI Act kent immers een breed werkingsgebied: niet alleen ontwikkelaars, maar ook gebruikers vallen onder deze wetgeving.

Het belang om applicaties bij de Wijzigings Advies Commissie (WAC) in te dienen wordt daardoor alleen nog maar groter. De WAC zal moeten beoordelen of er sprake is van gebruik van AI in een applicatie en daarover moeten adviseren. Dat betekent wel dat er in deze commissie voldoende kennis over AI aanwezig moet zijn.

Keerzijde van de medaille is dat leveranciers vaak AI omarmen omdat de term AI de verkoop stimuleert. Soms is daarbij niet altijd sprake van gebruik van AI. Ondanks dat de leverancier van de applicatie pretendeert AI te gebruiken, is dit niet het geval en speelt voor de Gemeente de AI Act dus ook geen rol. Ook hiervoor geldt weer dat dit in het WAC onderkend moet worden.

5.2 Data ethiek: de AVG voorbij

Data-ethiek houdt in dat de organisatie nadenkt over hoe ze wil dat er met data wordt omgegaan. Data-ethiek geeft dus geen regels en voorschriften, maar bevordert dat de organisatie zelf kritisch nadenkt over wat goed is om te doen met data.

Data-ethiek is dus breder dan alleen persoonsgegevens, maar zal daar in onze gemeente vaak wel betrekking op hebben. De AVG biedt vanzelfsprekend een kader dat helpt om goed met persoonsgegevens om te gaan. Echter, de AVG kent veel open normen en bovendien gaan de technologische ontwikkelingen, zoals de boven beschreven AI, dermate snel dat niet alles met regelgeving kan worden opgelost. Data-ethiek komt daarbij te hulp door na te denken en met elkaar te bespreken hoe de gemeente om wil gaan met de enorme hoeveelheid data die zij heeft.

Binnen het team Concern Control is in 2024 een initiatief gestart om te kijken of en hoe data ethiek binnen onze gemeente leeft. Begin 2025 is de verkenning afgerond en heeft een presentatie binnen het team Concern Control plaats gevonden. De bevindingen worden meegenomen naar een projectgroep voor dit onderwerp waar ook een afgevaardigde van het team Concern Control deel aan neemt.