



Jaarverslag Functionaris voor Gegevensbescherming 2024

Gemeenten Ermelo, Harderwijk en Zeewolde en de gemeenschappelijke regeling Meerinzicht



Plaats: Ermelo, Harderwijk en Zeewolde
Datum: mei 2025
Steller: Eric van Kessel FG



Inhoud

Inleiding	3
Managementsamenvatting	3
2024 in retroperspectief	4
Artificial Intelligence (AI)	4
Bewustwording	4
Positionering privacyteam	5
Adviezen en projecten in 2024	5
Proceseigenaren	5
Datalekken	5
Rechten van betrokkenen	6
Wet politiegegevens (Wpg)	6
Nieuwe wetgeving	7
Artificial Intelligence Act (AI Act) ingegaan in 2024	7
Cyberbeveiligingswet (NIS2) gaat in in Q3-2025	7
Open data directive ingegaan in 2021	7
Afsluitend	7

Inleiding

De Algemene Verordening Gegevensbescherming (AVG) is in mei 2018 in werking getreden in alle landen van de Europese Unie. Iedere overheidsorganisatie is verplicht om een Functionaris voor Gegevensbescherming (FG) aan te stellen. De FG is een onafhankelijke toezichthouder die toezicht houdt op de toepassing en de naleving van de AVG. Een onderdeel van de werkzaamheden is een jaarlijkse rapportage over de bevindingen van de FG. Dit is het jaarverslag van de FG voor de organisaties Ermelo, Harderwijk, Zeewolde en Meerinzicht over het jaar 2024.

Het jaarverslag van de FG wordt ter informatie via de directie aangeboden aan de verschillende colleges van de gemeenten en het bestuur van Meerinzicht, zij zijn bij meer dan 95% van de verwerkingen van persoonsgegevens verwerkingsverantwoordelijk (bepaalt het doel en de middelen voor de verwerking van persoonsgegevens en is daarvoor verantwoordelijk). De colleges van de gemeenten en het bestuur van Meerinzicht dienen kennis te nemen van het jaarverslag en kunnen een uitspraak doen over de vermelde aandachtspunten voor 2025. Daarnaast kunnen de colleges het jaarverslag ter informatie aanbieden aan de gemeenteraden en het publiceren op de website van de gemeenten.

Managementsamenvatting

Bewustwording in de organisatie was ook in 2024 een van de belangrijkste aandachtspunten binnen de werkzaamheden van de FG. Na jaren intensief hiermee bezig te zijn geweest, zien we steeds vaker dat de organisatie zich in een vroeg stadium meldt bij het privacyteam. In geval er persoonsgegevens verwerkt gaan worden in een proces wordt advies ingewonnen en kan er geadviseerd worden over hoe de verwerking rechtmatig is. Door een goede samenwerking met Burgerzaken, Geo en BI, worden aanvragen voor het leveren van persoonsgegevens eerst getoetst op de wettelijke bepalingen van de AVG en BRP, voordat er gegevens wel of niet geleverd worden.

Artificial Intelligence is in 2024 een belangrijk onderwerp geworden. In eerste instantie het gebruik binnen de organisatie van Large Language Models (LLM) als Gemini en ChatGPT. Voor het gebruik zijn richtlijnen opgesteld. Er blijft wel een risico dat een LLM foutief gebruikt wordt, of dat de richtlijnen verkeerd geïnterpreteerd worden. Op een aantal plaatsen in de organisatie worden eerste pilots gestart met het gebruik van algoritmen vanuit een efficiency oogpunt. De coördinatie hiervan is een belangrijk aandachtspunt en zal in 2025 moeten worden belegd. Risico is, als de coördinatie niet belegd is, dat er stappen worden gezet op het gebied van AI waarbij de consequenties onvoldoende in kaart zijn gebracht. Daarbij gaat het niet alleen om persoonsgegevens, maar ook om bedrijfsgevoelige informatie.

Er is in 2024 een stap gezet om meer duidelijkheid te creëren organisatie breed met betrekking tot proceseigenaarschap, wie heeft welke verantwoordelijkheid en exact waarvoor? Dit proces blijkt complexer dan verwacht, omdat er veel afstemming nodig blijkt te zijn in wat 'proceseigenaarschap' daadwerkelijk inhoudt. De definitie van een proceseigenaar is opgezet, maar nog niet geaccepteerd. Zonder het duidelijk hebben van proceseigenaren, lopen we als EZM een behoorlijk risico. Doordat proceseigenaren te ver van de praktijk staan, zien we dat compliance met de AVG niet altijd tot stand komt. Vanuit privacy is bijvoorbeeld de proceseigenaar randvoorwaardelijk voor het kunnen onderhouden van een verwerkingsregister. Ook voor de komende Cyberbeveiligingswet zijn proceseigenaren randvoorwaardelijk.

Er komen vanuit de EU een behoorlijk aantal nieuwe wetgevingen op gemeenten af. De belangrijkste op dit moment zijn de AI-act en de NIS2 (Cyberbeveiligingswet). Deze wetgeving gaat meer van de organisatie vragen op het gebied van compliance. De verwachting is dat de Cyberbeveiligingswet in het 3^e kwartaal van 2025 in werking zal treden. Om aan te kunnen tonen dat EHZM voldoet aan de eisen vanuit deze wet, zal er in 2025 veel werk verzet moeten worden.

2024 in retroperspectief

Artificial Intelligence (AI)

In het afgelopen jaar is kunstmatige intelligentie meer op de agenda gezet. In het voorjaar van 2024 heeft de netwerkdirecties meerdere informatiesessies gehad over hoe AI ingezet wordt en kan worden, over het gebruik van Large Language Models, en de juridische verplichtingen en risico's die gepaard gaan met AI. De eerste stappen zijn gezet in het verkennen van de mogelijkheden van AI voor de bedrijfsvoering van EHZM. Privacy & Informatieveiligheid heeft hier een bijdrage aan geleverd. De risico's van AI worden hierin ook meegenomen. Het belangrijkste is dat AI gecoördineerd in de organisatie wordt gerealiseerd. Bij gebruik van algoritmen komt er een verplichting om deze vast te leggen en openbaar te maken. Het risico is dat bij een versnipperd gebruik dit soort verplichtingen (naast privacy en informatieveiligheid) niet worden nagekomen. Vanuit de AI-act kan dit tot boetes leiden. Belangrijker is natuurlijk de betrouwbaarheid van de overheid. We hebben de verplichting naar de inwoners om verantwoording af te leggen over het gebruik van AI. Belangrijke uitgangspunten moeten zijn: voorkomen van discriminatie, vooroordelen die door het algoritme worden uitvergroot en geen geautomatiseerde besluitvorming.

De coördinatie is op dit moment nog niet geregeld. Er zijn op verschillende afdelingen al AI-projecten opgestart. Vanaf 1 februari 2025 moeten conform de AI-Act alle organisaties die iets met AI doen AI-geletterd zijn. Dit houdt in dat medewerkers op de hoogte moeten zijn van de risico's van AI in het gebruik. Daarnaast moet er op iedere toepassing een risicoanalyse worden uitgevoerd. In 2024 heeft het privacy team bij alle informatiebijeenkomsten aandacht besteed aan de risico's van AI. Er zijn richtlijnen uitgebracht voor het gebruik van LLM's.

Bewustwording

In 2024 is er opnieuw fors ingezet op het bewust maken van de medewerkers binnen de organisatie op het gebied van privacy & informatieveiligheid. Een kleine 250 medewerkers hebben een training gevolgd in 2024. In de jaren 2021 tot en met 2024 hebben ongeveer 900 medewerkers een training gevolgd. De trainingen in 2024 zijn gegeven aan nieuwe medewerkers, waarbij er een verplichting is om deel te nemen (ook voor tijdelijke medewerkers). Daarnaast hebben we een gedeelte van de medewerkers van de gemeente Ermelo in training gehad. De overige medewerkers van de gemeente Ermelo volgen de training in 2025. Ook het college van de gemeente Harderwijk heeft een training gevolgd. Tot slot zijn er informatiesessies geweest voor Burger- & Publiekszaken van alle 3 gemeenten. Ook in het Wpg-domein is er training geweest voor Boa's in 2024.

De bewustwording leidt in ieder geval tot bereidheid van het melden van datalekken en tot vragen in een vroeg stadium van nieuwe ontwikkelingen. Op beide vlakken is nog steeds verbetering mogelijk, maar het privacyteam wordt redelijk goed gevonden, als het gaat om vragen rondom de verwerking van persoonsgegevens.

Positionering privacyteam

Het privacyteam binnen EHZM is goed gepositioneerd binnen de organisatie. De FG is onafhankelijk en heeft geen andere taken binnen de organisatie en heeft directe toegang tot de verwerkingsverantwoordelijke organen. Dit is belangrijk, omdat daarmee de adviezen van de FG op het juiste niveau in de organisatie kunnen worden neergelegd en er geen sprake is van belangenverstrengeling.

Adviezen en projecten in 2024

In 2024 zijn er adviezen gegeven op een verscheidenheid van zaken. Een aantal hiervan: personeelsvolgsystemen, gezichtsscanners bij Burgerzaken, terugluisteren van telefoongesprekken bij KCC, juiste koppelingen met BRP bij Domein Sociaal, interne audit Wpg en de voorbereiding voor de externe audit, voorbereiding website advies, GBA-V project, beheer Justitieel Documentatie Systeem, camera's in de publieke ruimte, applicatiekeuze voor OOV.

Doordat het privacyteam steeds beter gevonden wordt en er meer aandacht is voor privacyaspecten vanuit het management, worden er vaker adviezen gevraagd in een vroeg stadium. Het grote voordeel daarvan is dat het privacyteam kan meedenken en kan zorgen dat de voorstellen voldoen aan de privacywetgeving.

Het privacy team heeft regelmatig overleg met verschillende disciplines in de organisatie (o.a. Concern Controllers, BRP specialisten, Boa's, BI-specialisten, Geo-specialisten, Duurzaamheid, Sociaal Domein, I&A). We hebben procedures ingericht waarbij aanvragen voor gebruik van persoonsgegevens eerst beoordeeld wordt door de afdeling (Burgerzaken, BI of Geo) en daarna door het privacyteam, voordat er uitvoering wordt gegeven aan de vraag. Dit is belangrijk om te voorkomen dat er persoonsgegevens worden verstrekt waar dat niet had gemogen (hetgeen in de praktijk in het verleden tot klachten van inwoners heeft geleid).

Proceseigenaren

Het is in 2024 niet gelukt om een start te maken met het inrichten van de organisatie op het gebied van proceseigenaren. Vanuit privacy & informatieveiligheid is dit een belangrijk probleem. Doordat er onvoldoende of geen proceseigenaren zijn is het niet mogelijk om het verwerkingsregister op orde te houden en is het niet eenvoudig om te voldoen aan de eisen van de ENSIA en BIO. Ook is het een handicap in het krijgen van overzicht op het gebied van de informatiehuishouding. Bij de cybersecurity oefening in het najaar van 2024 was dit ook een aandachtspunt. De complexiteit van de EHZM organisatie vraagt om een goede inrichting van dit fundament. Vanuit het perspectief van de FG is het van allergrootst belang om prioriteit te geven aan de inrichting van een structuur van proceseigenaren.

Datalekken

In 2024 zijn er in totaal 62 datalekken geregistreerd na melding van de organisatie. Een aantal gemelde datalekken waren na onderzoek geen datalek (10) en in een aantal gevallen waren het datalekken, maar van derde partijen (8). In 12 gevallen heeft er een melding plaatsgevonden bij de Autoriteit Persoonsgegevens (AP). Tot slot waren er 2 meldingen in het kader van de Wpg. In 24 gevallen hebben we een melding gedaan bij de betrokkene waarvan de data was gelekt. We melden vaker bij de betrokkene dan wettelijk noodzakelijk. De reden hiervoor is dat we tijdens informatiesessies van de deelnemers telkens horen dat ze altijd op de hoogte zouden willen worden

gesteld, als hun persoonsgegevens in een datalek voorkomen. Sinds 2023 worden daarom in meer gevallen de datalekken gemeld bij de betrokkene.

In onderstaande tabel staat de verdeling per organisatie:

Organisatie	Aantal datalek meldingen			
	2024		2023	
	Totaal	Gemeld AP	Totaal	Gemeld AP
Ermelo	5		8	
Harderwijk	9	1	16	3
Zeewolde	8	3	3	
Meerinzicht	40	8	43	7
Totaal	62	12	70	10

Ondanks meer bewustwording omtrent het onderwerp datalekken, worden nog niet alle datalekken gemeld (veelal onbewust). Tijdens de informatiesessies wordt regelmatig door deelnemers geconstateerd dat ze datalekken hebben gehad, maar deze niet als zodanig hadden herkend en dus niet gemeld. Blijvende aandacht voor het herkennen en melden van datalekken is daarom noodzakelijk. Wij geven altijd aan dat het melden van een datalek belangrijk is, maar dat het geen consequenties heeft voor de melder. Fouten worden nu eenmaal gemaakt. De meeste melders vinden het ook persoonlijk zeer vervelend als ze een datalek hebben veroorzaakt, zeker als het gaat om bijzondere persoonsgegevens. Hier is in een aantal gevallen nazorg nodig.

Rechten van betrokkenen

In 2024 zijn er 21 verzoeken van betrokkenen ontvangen. Een behoorlijke stijging ten opzichte van 2023, toen er 12 verzoeken van betrokkenen zijn ontvangen. Een mogelijke oorzaak van de toename in het aantal verzoeken is dat steeds meer inwoners bekend worden met de AVG en hun privacyrechten. Vooral het aantal klachten is in 2024 gestegen (van 2 naar 9). In een van de gevallen bleek de klacht ongegrond. In de overige gevallen had een deling van persoonsgegevens plaatsgevonden waar dat niet had gemogen. In al die gevallen hebben we intern maatregelen genomen om te voorkomen dat een dergelijke deling opnieuw gaat plaatsvinden. Een verdeling in de verzoeken in soort en organisatie staat in onderstaande tabel.

Soort	Ermelo	Harderwijk	Zeewolde	Meerinzicht	Wpg	Totaal	
						2024	2023
Inzage	2	2	2	3	1	10	8
Bezwaar op verwerking							2
Verwijdering			2			2	
Klacht	1	2	1	4	1	9	2
Totaal	3	4	5	7	2	21	12

Er zijn verschillende manieren waarop een inwoner inzage kan vragen (WOO-, BRP-, of AVG-verzoek). In de praktijk blijkt regelmatig dat deze mogelijkheden voor inwoners niet altijd duidelijk zijn, of dat ze verkeerd worden gebruikt. Om die reden zoeken we eerst contact met de aanvrager om te achterhalen wat het doel is van de bevraging. Op basis daarvan kunnen we meestal een betere invulling geven aan het verzoek.

Wet politiegegevens (Wpg)

In 2024 is de interne audit over 2023 uitgevoerd en bleek dat een aantal van de, in de externe audit geconstateerde tekortkomingen, opgelost waren. Veel van deze tekortkomingen waren zaken als

onvoldoende documentatie, of geen vastlegging van. Er is vooral in het Boa domein 1 veel werk verzet in het opstellen van procedures en procesbeschrijvingen. De samenwerking tussen de Boa's in EHZ op het gebied van de wijze van werken is verder geïntensiveerd. Privacy heeft de Boa's van Ermelo een training Wpg/AVG gegeven.

In 2024 hebben we één inzageverzoek en één klacht ontvangen. De klacht was terecht (een foto gedeeld op sociale media, herleidbaar naar de persoon) en heeft geleid tot een andere manier van werken. Er zijn 2 datalekken gemeld onder de Wpg; een is gemeld bij de AP, de andere niet.

In 2024 zijn de voorbereidende werkzaamheden voor de externe audit van dat jaar uitgevoerd; de daadwerkelijke audit zal in 2025 plaatsvinden.

Nieuwe wetgeving

Vanuit de EU zijn en worden er een groot aantal nieuwe wetgevingen ingevoerd. Het zijn allemaal wetten die betrekking hebben op de digitale wereld. Een aantal van deze wetgevingen heeft direct invloed op gemeenten (zie hieronder).

Artificial Intelligence Act (AI Act) ingegaan in 2024

De AI Act heeft als doel om een balans te hebben voor de bevordering van innovatie door het gebruik van AI, algoritmes en machine learning en aan de andere kant de bescherming van de rechten, de veiligheid en het welzijn van burgers en de maatschappij. De AI Act kent verboden voor systemen met een onaanvaardbaar risico en verplichtingen voor hoog risico systemen. De wet bevat regels over transparantie en aansprakelijkheid. Zowel vanuit de AI Act, als vanuit de AVG is er een verbod op geautomatiseerde besluitvorming. De wet treedt stapsgewijs in werking en zal op 2 augustus 2026 volledig van toepassing zijn.

Cyberbeveiligingswet (NIS2) gaat in in Q3-2025

De Cyberbeveiligingswet zal waarschijnlijk in het derde kwartaal van 2025 in Nederland worden aangenomen. Gemeenten moeten onder deze wet aan een groot aantal eisen gaan voldoen. Deels waren deze eisen al vanuit de BIO (Baseline Informatiebeveiliging) voor gemeenten aan de orde. De bestuurlijke verantwoordelijkheid en compliance wordt in deze wet belangrijker, waardoor de zorgplicht van overheidsorganisaties nadrukkelijker wordt.

Open data directive ingegaan in 2021

De Open Data Directive is bedoeld om af te dwingen dat overheidsinstanties bepaalde gegevens zoals gegevens over milieu, vervoer en overheidsdiensten die worden verzameld en beheerd, openbaar beschikbaar te stellen en hergebruiken. De wet is in 2021 ingegaan, maar in Nederland lopen we achter met het omzetten naar nationale wetgeving.

Afsluitend

Er zijn en worden binnen EHSM op het gebied van privacy & informatieveiligheid goede stappen gezet. De rol van het management en het bestuur op dit gebied is belangrijk. De bereidheid om het onderwerp regelmatig op de agenda te zetten is groot. Voor de goede uitvoering van de taken van de FG is dit een belangrijke voorwaarde. Het is een duidelijk compliment aan het management dat zij open staan voor aanbevelingen vanuit de FG om de organisatie op het gebied van privacy & informatieveiligheid robuuster en weerbaarder te maken. Dit laatste is ook zichtbaar in het vrijmaken van extra middelen om het security team structureel uit te breiden. Een hele belangrijke stap.

Er blijft natuurlijk ook nog veel te doen. De bewustwording op het gebied van informatieveiligheid en privacy is essentieel. En dat geldt voor alle lagen in de organisatie. Uiteindelijk wordt de kracht van de keten bepaald door de zwakste schakel. De eerste stappen op het gebied van oefenen met cybersecurity uitdagingen zijn in 2024 gezet. Het is belangrijk om deze in 2025 te continueren.

De Autoriteit Persoonsgegevens (AP) gaat in 2025 extra aandacht geven aan:

- Juiste positionering FG binnen overheidsorganisaties
- Algoritmes & AI (kunstmatige intelligentie)
- Inzageverzoeken: veel organisaties gaan niet correct om met inzageverzoeken, derhalve gaat de AP hier strenger op toe zien
- Cookies: nieuwe wetgeving geeft extra mogelijkheden om te handhaven. De AP gaat daarom strenger toezicht houden op het juist gebruik van cookies en cookiebanners
- Delen van persoonsgegevens binnen de overheid: in veel gevallen mogen persoonsgegevens niet gedeeld worden binnen de overheid. De AP gaat intensiever controleren op delingen
- Toezichtstrategie: de fundamentele waarden waar de AP bij de bescherming van persoonsgegevens prioriteit aan geeft zijn non-discriminatie, persoonlijke autonomie en vrijheid, controleerbaarheid en transparantie van de macht en de veiligheid van persoonsgegevens