Gemeente Almelo

Toezichtsplan 2024

Van de Functionaris Gegevensbescherming

Inleiding

De Functionaris Gegevensbescherming (FG) houdt toezicht op en adviseert over naleving van de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet AVG (UAVG) en de Wet politiegegevens (Wpg). Ook fungeert de FG als contactpunt voor de externe toezichthouder, de Autoriteit Persoonsgegevens (AP) en als aanspreekpunt voor betrokkenen, waaronder inwoners en medewerkers. Dit plan beschrijft hoe de toezichthoudende taak van de FG in 2024 wordt ingevuld.

Taken en positie van de FG

In de AVG en Wpg is een *verwerkingsverantwoordelijke* diegene of die partij die bepaalt met welk doel en met welke middelen persoonsgegevens verwerkt en beschermd worden. Alle bestuursorganen van de gemeente zijn zelf verwerkingsverantwoordelijke. Door de verwerkersverantwoordelijke worden management- en uitvoeringstaken gedelegeerd aan *proceseigenaren*, die op hun beurt verantwoordelijk zijn voor hoe dagdagelijks wordt omgegaan met persoonsgegevens. Een proceseigenaar gebruikt daarvoor middelen zoals beleid en systemen. De FG heeft een onafhankelijke positie binnen een organisatie en fungeert als intern toezichthouder, als verlengstuk van de AP. De FG rapporteert aan het hoogste bestuursorgaan en adviseert gevraagd en ongevraagd over de naleving van de AVG en Wpg. Hoewel deze adviezen formeel niet bindend zijn, gelden ze als zwaarwegend.

Daarnaast moet de verwerkingsverantwoordelijke het advies inwinnen van de FG bij de uitvoering van risico analyses voor gegevensverwerkingen, de Data Protection Impact Assessments (DPIA's). De FG adviseert over technische en organisatorische maatregelen om persoonsgegevens te beveiligen. Daarbij heeft de FG een aanjagende en informerende functie. De AVG schrijft voor dat bij een datalek de verwerkingsverantwoordelijke de FG dient te betrekken. De FG toetst het besluit van de verwerkingsverantwoordelijke of een datalek al dan niet gemeld wordt bij de AP en de betrokkene(n). Het melden van een datalek valt onder de verantwoordelijkheid van de verwerkingsverantwoordelijke. De FG is ook bevoegd om zelfstandig een datalek te melden.

Methoden van toezichthouden

Observatie

De FG monitort datalekken: kwantitatief, oorzaken, gevolgen en procesmatige aspecten zoals doorlooptijden. Het doel is tweeledig: vaststellen van het compliance niveau van de organisatie en het identificeren van verbetermogelijkheden in beleid en procedures. Daarnaast worden verzoeken van inwoners in het kader van AVG rechten, zoals verzoeken tot dossierinzage, gemonitord. Observatie van de fysieke werkomgeving vindt plaats door middel van waarnemings-rondes. Daarbij wordt gekeken naar informatieveilig gedrag, zoals het locken van beeldschermen en het verwijderen van (bakjes met) gevoelige informatie van de bureaus na een werkdag.

Interviews en teamgesprekken

In gesprekken met proceseigenaren en uitvoerend medewerkers worden mogelijke risico's voor informatieveiligheid en knelpunten in de bedrijfsvoering geïnventariseerd. Tevens worden het niveau van awareness en de ondersteuningsbehoefte vanuit de organisatie verkend. Want naast het duiden van het privacy-volwassenheidsniveau van de organisatie, is het evenzo belangrijk dat collega's zich gesteund voelen in het vinden van praktische oplossingen bij privacyrisico's.

Afwerken van standaard checklists

Hiervoor worden onder meer onderstaande tools gebruikt, die samen een GAP analyse opleveren:

- Borgingsproduct AVG 3.0 Toetsingskader (IBD), een inventarisatie van compliance op de AVG artikelen, tevens gehanteerd bij interne audits;
- CIPP Self Assessment om de positie op de Privacy volwassenheidsladder vast te stellen en een overzicht te genereren van de AVG-terreinen waarop nog extra aandacht nodig is;
- Checklist borging Wpg.

Documentatie onderzoek

- Steekproefsgewijs screenen van verwerkingsovereenkomsten en contracten met partijen die voor de Gemeente Almelo als verwerker optreden.
- Check op de correcte vastlegging van gegevensuitwisseling met partnerorganisaties en samenwerkingsverbanden, vanuit zowel AVG als Wpg.
- Steekproefsgewijs controleren van de rechtmatigheid van gegevensverwerkingen. Dat kan bijvoorbeeld door samen met een medewerker een proces te doorlopen.
- Vaststellen van uitvoering van beheersmaatregelen, zoals controle op logging, gebruik van beveiligd mailen, geheimhoudingsafspraken, et cetera.
- Analyse van relevante rapportages zoals de maandrapportages datalekken en AVG verzoeken, de Suwinet controles en (onderdelen uit) interne en externe audits.

Analyse, rapportage en advies

De stand van de organisatie in 2024 wordt gebruikt als nulmeting om van daaruit het ambitie-niveau en de bijbehorende consequenties voor de volgende jaren te laten vaststellen. Risico's, afwijkingen en complexe casuïstiek worden door de FG zo snel mogelijk gecommuniceerd met de proceseigenaren. Over het globale beeld met betrekking tot compliance, incidenten en verzoeken wordt met een kwartaalrapportage gerapporteerd aan management en bestuur.

Uitgelichte thema's in 2024

	Onderwerp	Methodiek/aanpak	Focus
1	Verwerking van persoonsgegevens in het kader van samenwerkingsverbanden	Interview, Observatie, Doc.onderzoek	Q2
2	Verantwoord gebruik algoritmes en Artificial Intelligence	Interview, Doc.onderzoek	Q4
3	Toezicht op uitvoering van DPIA's bij nieuwe verwerkingen (m.n. bij project/ procesmanagement)	Interview, Observatie Doc.onderzoek	Continu
4	Toezicht op doelbinding binnen AVG en Wpg	Doc.onderzoek	Q3
5	Controle op noodzakelijkheid en rechtmatigheid van verwerkingen	Toetsing DPIA's Interview, Observatie	Q3
6	Controle op vernietiging en rectificatie politiegegevens	Interview, Doc.onderzoek	Q4
7	Toezicht op logging en controle van de logging	Interview, Doc.onderzoek	Q2, Q1 '25
8	Toezicht op planning en uitvoering van AVG en Wpg audits	Interview, Observatie Doc.onderzoek	Q2, Q4
9	Toezicht op uitvoering rechten van betrokkenen	Interview, Observatie Doc.onderzoek	Q2, Q1 '25
10	Toezicht afhandeling datalekken	Observatie, Doc.onderzoek	Continu
11	Toezicht op naleving van Wpg en AVG	Interview, Observatie Doc.onderzoek	Continu

Pro memori (vanaf 2025)

Voor een aantal onderwerpen is actief toezicht nog niet haalbaar. Het is bijvoorbeeld niet realistisch om te rapporteren over het effect van privacy bewustzijnstrainingen, omdat een doelgroepgericht awareness programma op de rol staat voor 2025. Ook wordt op dit moment het register van verwerkingsactiviteiten nader ingericht. Aan de hand van de daaruit geïdentificeerde risico's wordt beoordeeld welke DPIA's uitgevoerd moeten worden. Met die risicogestuurde prioritering wordt de organisatie in staat gesteld om meer regie te voeren. Voor nieuwe verwerkingen en projecten worden overigens, conform wettelijke verplichting, wel DPIA's uitgevoerd. Gedurende het jaar 2024 wordt aan het eind van ieder kwartaal de voortgang op deze onderwerpen gemonitord, bijzonderheden worden gemeld in de kwartaalrapportage van de FG.