

**Jaarverslag 2023 van
de Functionaris
Gegevensbescherming**

Inhoud

INLEIDING EN LEESWIJZER	3
MANAGEMENTSAMENVATTING	4
TERUGBLIK 2023	5
1. Beleid	5
Aanbevelingen	5
2. Processen	5
Aanbevelingen	5
3. Organisatie	6
Aanbevelingen	6
4. Rechten van betrokkenen	6
Aanbevelingen	6
5. Beveiliging	67
Aanbevelingen	7
6. Samenwerking	7
Aanbevelingen	7
7. Verantwoording en audits	7
Aanbevelingen	8
EINDWOORD	8
BIJLAGE 1: AANBEVELINGEN	9

Inleiding en leeswijzer

De gemeente Almelo verwerkt bij de uitvoering van haar taken vele (gevoelige) gegevens van veel (kwetsbare) inwoners binnen de verschillende domeinen, maar ook van haar medewerkers, burgers uit andere gemeenten en externen.

Met de komst van de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg), zijn er wettelijke kaders of instructies beschreven waar de verwerkingen van persoons- en politiegegevens aan moeten voldoen.

De implementatie van deze kaders, maar ook het kunnen aantonen daarvan, vraagt veel van de organisatie. Een van de wettelijke vereisten is het aanstellen van een Functionaris Gegevensbescherming (FG).

De FG adviseert over en houdt toezicht op het naleven van de vereisten uit de AVG en Wpg. In dit jaarverslag breng ik verslag uit van de verrichte werkzaamheden in 2023 om te voldoen aan de AVG en de Wpg en geef ik u mijn bevindingen en aanbevelingen.

Het jaarverslag is opgedeeld in een managementsamenvatting, een terugblik op 2023 uitgesplitst in 7 verschillende thema's en een eindwoord. In de uitwerking per thema geef ik ook mijn aanbevelingen. De 7 verschillende thema's zijn:

1. Beleid
2. Processen
3. Organisatie
4. Rechten van betrokkenen
5. Beveiliging
6. Samenwerking
7. Verantwoording en audits

Afsluitend zijn de genoemde aanbevelingen opgenomen in bijlage 1.

Managementsamenvatting

Organisatie

In 2023 is er aandacht geweest voor het (opnieuw) leggen van een stevige basis op het gebied van de bescherming van persoons- en politiegegevens.

Door te weinig capaciteit en het hebben van prioriteit bij het draaiende houden van de organisatie, is er in voorgaande jaren te weinig ruimte geweest voor het onderhoud en verdere implementatie van deze basis.

In 2023 is het privacyteam daarom uitgebreid met extra capaciteit, waarbij er een duidelijke scheiding is aangebracht binnen de functies van Privacy Officer en Functionaris Gegevensbescherming. Daar waar in de eerste helft nog veel werkzaamheden door externe medewerkers waren uitgevoerd, staat er eind 2023 een team van interne medewerkers.

Werkzaamheden

In 2023 zijn er meerdere beleidsstukken en procedures her-/geschreven, om zodoende de organisatie duidelijke kaders te geven waarbinnen het kan opereren.

Er is een start gemaakt met het in kaart brengen van alle verwerkingen, waarbij het register met verwerkingen van politiegegevens inmiddels compleet is. Ook is er veel werk verzet om aan de wettelijke normen voor het verwerken van politiegegevens te voldoen.

Er zijn echter ook een aantal zaken waar de gemeente in 2023 niet aan toegekomen is. De gemeente Almelo loopt achter met het uitvoeren van de wettelijk verplichte risico-analyses op verwerkingen met een hoog risico voor betrokkenen. De inhaalslag op deze achterstand moet zo snel mogelijk plaatsvinden.

Ook zijn er amper bewustzijns campagnes op het gebied van privacy (en informatiebeveiliging) uitgevoerd; het belang van dit soort campagnes is groot omdat het menselijk handelen het grootste risico op incidenten is.

Risicovolle dossiers

Vanuit mijn rol als Functionaris Gegevensbescherming heb ik in 2023 mijn zorgen geuit en geadviseerd over 2 dossiers betreffende samenwerkingen. Ik wil de gemeente Almelo graag adviseren om meer zicht en grip te krijgen op de vele samenwerking(sverband)en waar gemeente Almelo bij betrokken is.

Terugblik 2023

1. Beleid

In 2023 is veel werk verzet in het opstellen of actualiseren van verschillende beleidsstukken op het gebied van de AVG en Wpg. Zo is er een nieuw overkoepelend privacybeleid opgesteld, een operationeel beleid Wpg en een tactisch informatiebeveiligingsbeleid.

Daarnaast zijn er meerdere procedures en werkinstructies uitgeschreven, bijvoorbeeld procedures voor de afhandeling van AVG-verzoeken, het uitvoeren van Data Protection Impact Assessments (DPIA's) en werkinstructies hoe om te gaan met politiegegevens.

Dit geeft de organisatie handvatten in de omgang met gevoelige gegevens.

Maar het brengt de organisatie ook naar een hoger volwassenheidsniveau doordat uniformer en daarmee efficiënter gewerkt kan worden.

Aanbevelingen

Met de nieuwe beleidsstukken (opzet), is het aan te raden om in 2024 een gap-analyse uit te voeren om zodoende te achterhalen welke zaken nog geïmplementeerd moeten worden om de realiteit dichterbij de gewenste situatie te brengen (bestaan en werking).

2. Processen

Verwerkingen van persoons-/ of politiegegevens dienen te voldoen aan de AVG of Wpg. Een belangrijk handvat hierbij is het (wettelijk verplichte) register van verwerkingen.

Begin 2023 is gebleken dat het huidige register niet volledig, actueel en/of juist was. Hierop volgend is het register van verwerkingen onder de Wpg opgesteld.

Ook is een plan van aanpak gemaakt voor het actualiseren en completeren van het register van verwerkingen onder de AVG. In 2024 zal dit plan uitgevoerd worden.

Op verwerkingen met een hoog risico voor betrokkenen moet een risico-analyse, de DPIA uitgevoerd worden, vóór aanvang van de verwerking. Helaas is geconstateerd dat er een achterstand is in de uitgevoerde DPIA's.

In 2023 is een procesbeschrijving opgesteld voor het uitvoeren van een DPIA en is er gestart met het ontwerp van een format voor de DPIA (oplevering in Q1 2024).

Ook is er een presentatie gemaakt om dit proces en het belang aan alle stakeholders uit te leggen. Het informeren van de organisatie start in de eerste helft van 2024.

Aanbevelingen

In het plan van aanpak staan ook adviezen over de borging van de registers van verwerkingen. Houdt de aandacht op deze adviezen, zodat de gemeente niet alleen in 2024 actuele en juiste registers hebben, maar ook in de daaropvolgende jaren.

De verantwoordelijkheid van het uitvoeren van DPIA's ligt bij de procesverantwoordelijken; de Privacy Officers kunnen hierbij ondersteunen.

Zorg dat in 2024 de verantwoordelijken voldoende middelen vrijmaken om een inhaalslag op de DPIA's te kunnen maken.

3. Organisatie

Begin 2023 vertrok de interne Privacy Officer en tevens waarnemend FG bij de gemeente Almelo. De positie van Privacy Officer is in 2023 met 1,5 fte ingevuld met vaste medewerkers.

Daarnaast zijn er verschillende opdrachten op het gebied van privacy en politiegegevens door externe medewerkers uitgevoerd.

Er is een duidelijke scheiding tussen Privacy Officer en FG aangebracht; de positie van FG is in 2023 extern vervuld. Eind 2023 is een geschikte kandidaat gevonden om de positie van FG in 2024 intern te gaan vervullen.

In 2023 zijn er amper tot geen bewustzijns campagnes uitgevoerd op het gebied van Privacy en Informatiebeveiliging. Het belang om hier verandering in te brengen is groot; de grootste risicofactor op deze gebieden is het menselijk handelen.

Aanbevelingen

Zorg voor een structureel bewustzijns campagne en stel hier voldoende middelen voor beschikbaar.

Zorg voor voldoende capaciteit binnen het Privacy Officers team; 1,5 fte is niet genoeg voor een organisatie als gemeente Almelo. Dit kan tijdelijk opgevuld worden met externe opdrachten. Zodra de basis op het gewenste volwassenheidsniveau is, evalueer en bepaal het aantal gewenste Privacy Officer fte.

4. Rechten van betrokkenen

Betrokkenen hebben onder de AVG en Wpg recht om zowel actief als passief geïnformeerd te worden over de verwerking van hun gegevens.

Eind 2023 is daarom gestart met het actualiseren van de privacyverklaring op de website.

Ook zijn er een nieuwe procedures opgesteld die voorzien in de afhandeling van inzage- en verwijderingsverzoeken van betrokkenen.

Het is gebleken dat er veel tijd kwijt gaat aan het handmatig doorzoeken van de systemen voor het ophalen van de informatie bij dergelijke verzoeken. Hierdoor zijn in meerdere gevallen de verzoeken niet binnen de wettelijke termijnen afgehandeld.

In 2023 is gekeken of het doorzoeken van de systemen geautomatiseerd kon worden. Dit onderzoek is voortijdig gestopt vanwege onvoldoende capaciteit en/of prioriteit.

Aanbevelingen

Zorg voor voldoende (juiste) capaciteit om het doorzoeken van de systemen te automatiseren en daarmee de wettelijke termijnen te waarborgen.

5. Beveiliging

In 2023 is er een verbeterplan op het gebied van informatiebeveiliging opgesteld. Hierin zijn onder andere de verbeterpunten uit de Wpg-audit opgenomen.

Ook is er een nieuwe procedure opgesteld en geïmplementeerd voor de afhandeling van beveiligingsincidenten, waaronder datalekken.

Datalekken en de afhandeling daarvan worden centraal geregistreerd. Er is echter, vanwege andere prioriteiten, nog geen (wettelijk verplicht) datalekregister.

Aanbevelingen

Zorg voor voldoende middelen voor het uitvoeren van het verbeterplan.

Zorg voor het opstellen van het datalekregister.

6. Samenwerking

In 2023 zijn er twee dossiers betreffende samenwerkingen in Twente geweest waar een aantal FG's gezamenlijk hun zorgen over hebben geuit aan de verschillende bestuursorganen. Dit betroffen zorgen over zowel de inhoud (processen/techniek) als over governance (het beleggen van rollen en verantwoordelijkheden).

Binnen de gemeente Almelo is gebleken dat er te weinig zicht is op de vele samenwerkingen, zowel met andere gemeenten en verwante partijen zoals politie en hulpverleners, als met dienstverleners.

Aanbevelingen

Breng in kaart alle verschillende samenwerkingen en neem deze op in het register van verwerkingen.

Inventariseer of alle benodigde verwerkersovereenkomsten aanwezig en actueel zijn. Zo niet, sluit deze (opnieuw) af.

Neem het toezicht houden op de samenwerkingen met de hoogste risico's voor betrokkenen op in het toezichtsplan 2024 van de FG.

7. Verantwoording en audits

Eind 2022 heeft de wettelijk verplicht Wpg-audit plaatsgevonden. Uit het rapport bleek dat de gemeente Almelo voor het overgrote deel niet voldeed aan de normen. In 2023 is er een verbeterplan opgesteld en uitgevoerd. Dit plan was met name gericht op opzet en bestaan. In november 2023 heeft de, wederom verplichte, heraudit. Hieruit bleek dat gemeente Almelo grote stappen heeft gezet in het voldoen aan de normen.

De gemeente Almelo heeft een eigen verantwoordingsplicht om aan te kunnen tonen dat de verwerkingen van persoonsgegevens voldoen aan de principes uit de AVG.

Hier zijn verschillende instrumenten voor, zoals bijvoorbeeld het borgingsproduct van de IBD, of de in 2023 door de AP goedgekeurde AVG-standaard BC 5701 van Brand Compliance (let op: de accreditatieaanvraag bij de Raad van Accreditatie loopt nog).

Aanbevelingen

Blijf aandacht houden voor de verdere implementatie van de Wpg-normen, ook op het gebied van bestaan en werking: de in- en externe audits blijven jaarlijks terugkomen.

Zodra de basisprincipes van de AVG op het gewenste volwassenheidsniveau zijn geïmplementeerd in de organisatie, implementeer een instrument waarmee het volwassenheidsniveau gemeten en aangetoond kan worden, en gestuurd kan worden op verdere verbeteringen.

Eindwoord

Ondanks de geringe middelen in het eerste half jaar van 2023, is er met name in het tweede half jaar veel werk verzet door het Privacyteam.

Daar waar er in 2023 nog veel werkzaamheden door externen werd uitgevoerd, zal er in 2024 een sterker intern team zijn wat ondersteund wordt door externe inzet.

De focus heeft in 2023 gelegen op het op orde brengen van de basis, kaders te stellen waarbinnen de organisatie kan opereren en het op orde brengen van het interne team. Dit terwijl de winkel tegelijkertijd draaiende gehouden moest worden. Hoewel de gemeente Almelo veel stappen heeft gezet in 2023, moeten er ook nog genoeg stappen genomen worden om op een volwassenheidsniveau te komen wat medewerkers en inwoners mogen verwachten van de gemeente Almelo.

Per 1 maart 2024 start mijn opvolgster in de functie FG. Na maart 2024 zitten mijn werkzaamheden binnen de gemeente erop.

Ik wil daarom als slot mijn vertrouwen in het huidige team en mijn opvolgster uitspreken; zij hebben zeker de kennis en kunde om gemeente Almelo te helpen bij de uit te voeren vervolgstappen, waarbij de geringe beschikbare capaciteit een blijvend aandachtspunt is.

Met vriendelijke groet,

Nynke Ruinard
Functionaris Gegevensbescherming

Bijlage 1: Aanbevelingen

Aanbevelingen	
Beleid	- Voer een gapanalyse uit op de beleidsstukken en zorg voor implementatie van de ontbrekende zaken.
Processen	- Borg dat de registers van verwerkingen ook na opzet actueel en juist blijven. - Zorg voor voldoende middelen om een inhaalslag met de DPIA's te kunnen maken.
Organisatie	- Zorg voor een structureel bewustzijns campagne - Zorg voor voldoende capaciteit binnen het Privacyteam -
Rechten van betrokkenen	- Zorg voor capaciteit om het doorzoeken van systemen naar persoonsgegevens te automatiseren
Beveiliging	- Zorg voor voldoende middelen voor het uitvoeren van het verbeterplan - Zorg voor het opstellen van een datalekregister
Samenwerking	- Breng alle samenwerkingen in kaart en neem deze op in de registers van verwerkingen - Inventariseer en sluit alle verwerkersovereenkomsten af - Neem toezicht op samenwerkingsverbanden op in het toezichtsplan 2024 van de FG
Verantwoording en audits	- Blijf aandacht houden voor verdere implementatie van de Wpg-normen - Implementeer een AVG borgingsinstrument