

## Reglement Functionaris voor gegevensbescherming Helmond 2026

De burgemeester van de gemeente Helmond en het college van burgemeester en wethouders van de gemeente Helmond ieder voor zover bevoegd,

gelet op het bepaalde in artikel 37, 38 en 39 van de Algemene verordening gegevensbescherming (AVG) en artikel 36 van de Wet politiegegevens (Wpg)

### BESLUIT:

Vast te stellen het Reglement Functionaris voor gegevensbescherming Helmond 2026.

#### Artikel 1. Definities

In deze reglement wordt verstaan onder:

- a. AI: artificial intelligence, zoals bedoeld in artikel 3 de EU AI-act;
- b. AVG: Algemene verordening gegevensbescherming;
- c. Ciso: Chief information security officer, verantwoordelijke voor de coördinatie van informatiebeveiliging, zoals bedoeld in de Baseline Informatiebeveiliging Overheid (BIO);
- d. DPIA: Data protection impact assessment, een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens, zoals bedoeld in artikel 35 van de AVG;
- e. Datalek: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, zoals bedoeld in artikel 4 lid 12 van de AVG;
- f. FG: Functionaris voor gegevensbescherming, toezichthouder op de verwerking van persoonsgegevens zoals bedoeld in afdeling 4 van de AVG en artikel 36 van de Wpg;
- g. NRRFG: Nederlands Register voor Functionarissen voor gegevensbescherming, het Nederlandse kwaliteitsregister voor FG's;
- h. SPO: Security en Privacy officer, hij/zij ondersteunt de organisatie bij het borgen van informatiebeveiliging en bescherming van persoons- en politiegegevens;
- i. Persoonsgegevens, alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (bijv. naam, adres, geboortedatum). Naast gewone persoonsgegevens zijn er ook bijzondere persoonsgegevens. Die gaan over gevoelige onderwerpen, bijvoorbeeld etnische achtergrond, politieke voorkeuren en de gezondheid, zoals bedoeld in artikel 4 lid 1 van de AVG;
- j. Politiegegevens: een persoonsgegeven dat verwerkt wordt in het kader van de opsporingstaak. Zoals bedoeld in artikel 1 onder 1 van de Wet politiegegevens. Een politiegegeven is een specifieke versie van een persoonsgegeven;
- k. Portefeuillehouder: het collegelid met privacy in de portefeuille;
- l. Verwerkingsverantwoordelijke: de in artikel 3 lid 1 genoemde bestuursorganen;
- m. Wpg: Wet politiegegevens.

#### Artikel 2. Doel van het reglement

Voor het goed kunnen functioneren als FG zijn een aantal zaken (aanwijzing, positie en taken) in de wet vastgelegd. Bijzondere aandacht daarbij verdient de onafhankelijke rol en dus de autonomie van de FG. Dit reglement bevat de noodzakelijke kaders om de autonomie en de onafhankelijkheid van de FG te waarborgen, zodat hierover in de organisatie geen misverstanden kunnen ontstaan.

#### Artikel 3 Verantwoordelijkheid

1. Het college van burgemeester en wethouders en de burgemeester als bestuursorgaan zijn ieder voor hun eigen bevoegdheid verantwoordelijk voor de naleving van de privacywetgeving bij de verwerking van persoonsgegevens.
2. De in lid 1 genoemde bestuursorganen zorgen ervoor dat zij de naleving van de privacywetgeving kunnen aantonen. Zij worden hierover geadviseerd door de FG.
3. De in lid 1 genoemde bestuursorganen wijzen een ambtelijk functionaris aan als FG, zoals bedoeld in de artikelen 37-39 van de AVG én als bedoeld in artikel 36 van de Wpg.

#### **Artikel 4. Positie van de FG**

1. De FG ontvangt geen aanwijzingen of instructies over hoe de functie van de FG wordt uitgeoefend of hoe een bepaalde aangelegenheid moet worden behandeld. Dit betekent dat er geen sprake is van een interne opdrachtgever-opdrachtnemer relatie.
2. De FG krijgt geen taken of functies die leiden tot belangenverstrengeling tussen deze taken of functies. Dit betekent dat de FG binnen de gemeente Helmond geen taken of functies uitvoert waarin hij/zij doel en middelen van de gegevensverwerking bepaalt. In ieder geval voor de volgende functies en taken geldt dat ze niet door de FG kunnen worden uitgevoerd:
  - a. managementfuncties;
  - b. CISO;
  - c. SPO;
  - d. AI compliance officer;
  - e. het opstellen van een verbeterplan privacy;
  - f. het opstellen van privacybeleid en overeenkomsten;
  - g. het namens de gemeente Helmond optreden bij geschillen of andere aangelegenheden;
  - h. het opstellen van een risico analyse (waaronder een DPIA);
  - i. het uitvoeren van een Wpg audit.
3. De FG is rechtstreeks onder de gemeentesecretaris gepositioneerd. De FG is onderdeel van het team concern control. Er worden met hem/haar geen functioneringsgesprekken gevoerd waarin instructies worden gegeven over zijn/haar functioneren.
4. De FG ondervindt geen nadelen die samenhangen met zijn/haar optreden als FG. Zoals (dreiging van) sancties (waaronder het uitstellen van promotie, het verhinderen van verdere carrière uitbouw, het weigeren van voordelen die andere werknemers wel genieten) of ontslag. Dat laat onverlet dat de FG nog steeds rechtmatig kan worden gesanctioneerd of ontslagen om andere redenen die niet te maken hebben met zijn/haar optreden als FG.
5. De FG geeft mogelijke conflicten van belangen direct door aan de gemeentesecretaris of aan het in artikel 3 lid 1 genoemde toepasselijke bestuursorgaan.

#### **Artikel 5. Middelen**

De verwerkingsverantwoordelijke verstrekt voldoende middelen aan de FG om zijn/haar taken uit te kunnen voeren. Het volgende wordt hierbij in aanmerking genomen:

1. De FG actief wordt ondersteund door de in artikel 3 lid 1 genoemde bestuursorganen en het management. Ze heeft daarom rechtstreeks toegang tot de gemeentelijke bestuursorganen, de gemeentesecretaris en de directie. Ook heeft de FG toegang tot alle college- en directievoorstellen.
2. De organisatie beschikt over een centraal team van SPO's. Ook binnen de afdelingen is voldoende capaciteit aanwezig om de kwaliteit van de gegevensbescherming te borgen.
3. De FG krijgt voldoende tijd om de werkzaamheden uit te voeren. Hierbij wordt rekening gehouden de volwassenheid van de organisatie en het feit dat er binnen de gemeente veel gevoelige en complexe gegevensverwerkingsactiviteiten plaatsvinden.
4. De FG krijgt voldoende gelegenheid krijgt om zich te ontwikkelen en om op de hoogte te blijven van nieuwe ontwikkelingen op het gebied van gegevensbescherming.
5. De FG ontvangt adequate ondersteuning op het vlak van financiële middelen en infrastructuur (faciliteiten en apparatuur).

#### **Artikel 6. Betrekken van de FG**

1. De FG wordt zo vroeg mogelijk betrokken bij alle aangelegenheden die de gegevensbescherming raken.
2. De FG wordt betrokken bij vergaderingen van het management en wordt uitgenodigd en geraadpleegd bij datalekken en beslissingen met gevolgen voor gegevensbescherming.
3. Met de gemeentesecretaris vindt periodiek overleg plaats. Tijdens dit overleg worden actuele ontwikkelingen en de naleving van de privacywet- en regelgeving besproken.
4. De FG wordt betrokken bij bestuurlijke behandelvoorstellen die de bescherming van persoons- en/of politiegegevens raken. Op de stukken die worden aangeleverd voor de collegevergadering is altijd aangegeven of het voorstel (beleidsmatig) raakt aan het verwerken van persoonsgegevens en of een SPO-er dan wel de FG in dat kader heeft geadviseerd.
5. Met de portefeuillehouder vindt periodiek overleg plaats. Tijdens dat overleg wordt het toezichtplan en de rapportages van de FG besproken. Ook wordt de voortgang besproken van de activiteiten die organisatie verricht om aan de privacywet- en regelgeving te voldoen.
6. Voor formele overleggen van het management (directieraad en / of MT-overleg binnen de sectoren) hanteert de gemeente in het algemeen een standaard format voor agendering en besluitvorming van voorstellen of bespreekpunten. In deze formats wordt door het management standaard de vraag opgenomen of het voorstel (beleidsmatig) raakt aan het verwerken van persoonsgegevens en / of de FG in dat kader heeft geadviseerd.

7. Management en bestuursorganen, nemen het advies van de FG naar behoren in overweging. Dit betekent dat:
  - a. de FG schriftelijk advies uitbrengt, dit advies zwaarwegend is en daarom normaliter wordt opgevolgd;
  - b. wanneer er toch wordt afgeweken van het FG advies, dit schriftelijk en gemotiveerd gebeurt, én de FG vooraf wordt geïnformeerd, en;
  - c. het advies van de FG wordt toegevoegd aan college- en directievoorstellen, en;
  - d. het FG-advies en (indien aan de orde) het besluit om af te wijken van dit advies worden gearchieveerd, conform de archiefwet en net zo lang worden bewaard als de stukken waar het advies betrekking op heeft.
8. Als bij een college- of directievoorstel het ambtelijk advies afwijkt van het advies van de FG, kan de FG worden uitgenodigd voor het directieoverleg of het BOW waar het collegevoorstel wordt besproken.
9. De directie bespreekt elk kwartaal de afwijkingen op de FG adviezen. De FG wordt voorafgaand aan dit overleg uitgenodigd om zijn/haar mening te geven over de motivering van de afwijking.

### **Artikel 7 Taken van de FG**

De FG heeft bij wet bepaalde werkzaamheden. Deze werkzaamheden zijn in deze regeling nader uitgewerkt en omvatten in ieder geval, maar niet uitsluitend:

1. Adviseren

De FG ziet toe op naleving van de privacywet- en regelgeving en brengt advies uit over de risico's van bestaande verwerkingen en voorgenomen nieuwe producten en diensten. Het advies is een vorm van preventief toezicht. De FG prioriteert zijn/haar activiteiten en inspanningen en richt zich daarbij op zaken die een hoger risico voor de gegevensbescherming inhouden en daarmee een grote impact hebben op de samenleving en/of de organisatie.

  - a. De FG adviseert en informeert gevraagd en ongevraagd de verwerkingsverantwoordelijke en haar werknemers over hun verplichtingen bij de verwerking van persoons- en politiegegevens.
  - b. De FG adviseert zowel op bestuurlijk- en concernniveau als op managementniveau over hoe aan deze verplichtingen kan worden voldaan.
  - c. De FG adviseert zowel op bestuurlijk- en concernniveau als op managementniveau over de daartoe benodigde organisatorische inrichting.
  - d. De FG adviseert over beleids- en beheerinstrumenten, kaders en programma's ter optimalisering van de organisatiesturing en bedrijfsvoering op het gebied van een veilige verwerking van persoons- en politiegegevens in overeenstemming met wet- en regelgeving.
  - e. De FG adviseert over, en draagt daarmee bij aan, strategisch, tactisch en operationeel beleid op het gebied van de naleving van privacywet- en regelgeving.
  - f. De FG adviseert over de impact die een digitale crisis heeft op de eerbiediging van de persoonlijke levenssfeer. Zij/hij neemt daarom als adviseur deel aan een crisisteam in het geval van een dergelijke digitale crisis.
  - g. De FG volgt ontwikkelingen die van invloed (kunnen) zijn op de eerbiediging van de persoonlijke levenssfeer, zoals de impact van digitalisering en digitale innovaties op de privacy van betrokkenen. Daarnaast volgt ze de ontwikkelingen van Europese en landelijke wet- en regelgeving op het gebied van privacy en digitalisering. Hij/zij vertaalt deze ontwikkelingen in adviezen over de naleving van privacywet- en regelgeving.
  - h. De FG adviseert de organisatie met betrekking tot opleiding en een bewustwordingsprogramma op het gebied van privacy.
  - i. De FG adviseert over de risico's van bestaande verwerkingen en voorgenomen nieuwe producten en diensten. Het gaat daarbij om:
    - i. de afweging om wel of niet een risicoanalyse, waaronder een DPIA uit te voeren, en
    - ii. de onderzoeksmethode die geschikt is voor het uitvoeren van de risicoanalyse, en
    - iii. de vraag of de organisatie de risico analyse zelf uitvoert, of hiervoor een gespecialiseerd bureau inschakelt, en
    - iv. of de risicoanalyse juist is uitgevoerd, en
    - v. de waarborgen die nodig zijn om de privacyrisico's te beperken, en
    - vi. de vraag of de uitkomsten van de risicoanalyse in overeenstemming zijn met de wet- en regelgeving, en
    - vii. of de Autoriteit Persoonsgegevens (AP) eerst moet worden geraadpleegd.
2. Toezicht
  - a. De FG ziet toe op de naleving van de AVG en de Wpg.
  - b. De FG ziet toe op de naleving van intern vastgesteld beleid op het gebied van de bescherming van persoons- en politiegegevens.

- c. De FG ziet toe op het melden en mededelen van inbreuken op de informatiebeveiliging in verband met persoonsgegevens (datalekken).
  - d. De FG rapporteert zijn/haar bevindingen op bestuurlijk-, concernbreed- en/of management-niveau en doet (gevraagd en ongevraagd) relevante aanbevelingen en verbetervoorstellen op operationeel, tactisch en/of strategisch niveau.
  - e. De FG stelt jaarlijks een toezichtplan op. Het plan geeft weer waar het toezicht op de verwerking van persoons- en politiegegevens zich in het komende jaar op richt.
  - f. De FG heeft, in relatie tot zijn/haar taken, de bevoegdheid om inlichtingen en inzage te vragen en om zaken te onderzoeken. Om dit mogelijk te maken:
    - i. heeft de FG (ongevraagd) toegang tot alle ruimten waar een verwerking van persoonsgegevens plaatsvindt, en
    - ii. heeft de FG toegang tot registers inzake verwerking van persoons- of politiegegevens en registers inzake inbreuken in de informatiebeveiliging waar al dan niet persoonsgegevens bij zijn betrokken, en
    - iii. heeft de FG toegang tot alle collegevoorstellen en directievoorstellen, en
    - iv. is de FG bevoegd om apparatuur, programmatuur, gegevensbestanden, boeken en bescheiden in te zien, hier kopieën van te maken en deze te onderzoeken, en
    - v. is de FG bevoegd zich de werking van apparatuur en programmatuur te doen tonen, en
    - vi. verstrekken de verantwoordelijke en de personen die bij een verwerking van persoonsgegevens of politiegegevens zijn betrokken desgevraagd aan de FG alle inlichtingen die de FG voor de uitoefening van de taak nodig heeft, en
    - vii. verlenen de hiervoor genoemde personen alle overige medewerking, en
    - viii. kan de FG voor het onderzoek gebruik maken van de diensten van derden, indien de FG dit naar redelijkheid nodig acht.
  - g. De FG maakt van zijn/haar bevoegdheden slechts gebruik voor zover dat redelijkerwijs voor de vervulling van zijn/haar taak nodig is.
3. Rapporteren
- a. De FG rapporteert jaarlijks aan de gemeenteraad en aan het college van burgemeester en wethouders en burgemeester over zijn/haar werkzaamheden en zijn/haar bevindingen over de naleving van de privacy wet- en regelgeving. .
  - b. Een publieksvriendelijke versie van de rapportage wordt in- en extern gepubliceerd.

### **Artikel 8. Vertrouwelijkheid**

In het kader van vertrouwelijkheid zal de FG:

1. alle informatie die in het kader van zijn functie wordt verkregen vertrouwelijk en zorgvuldig behandelen;
2. informatie delen, indien hiervoor een wettelijke verplichting bestaat, de betrokkene toestemming heeft gegeven of wanneer een rechter daartoe opdracht geeft;
3. zich ook na beëindiging van dienstverband of opdracht, houden aan de vertrouwelijkheid en geheimhouding die van kracht was.
4. Lid 1 verhindert de FG echter niet om met de AP of externe deskundigen contact op te nemen en om advies te vragen.

### **Artikel 9. Toegankelijkheid en samenwerking.**

1. De FG treedt op als contactpunt voor en werkt samen met de Autoriteit Persoonsgegevens.
2. De FG is binnen en buiten de organisatie het aanspreekpunt voor vragen, klachten en signalen met betrekking tot gegevensbescherming. Daarbij hoort dat hij/zij benaderbaar is voor betrokkenen met name in verband met uitoefening van hun rechten. Hiertoe worden de contactgegevens van de FG op de gemeentelijke en op de interne website geplaatst.
3. De FG adviseert de organisatie over de afhandeling van klachten ten aanzien van de verwerking van persoons- of politiegegevens. Desgewenst kan de FG een onafhankelijke bemiddelende rol spelen in de oplossing van een klacht.
4. De FG werkt samen met de Ciso, Concern control en de auditor op de thema's informatiebeveiliging en risicomanagement.
5. De FG werkt samen met vertrouwenspersonen, de coördinator en de adviseur integriteit & Sociale Veiligheid, voor zover het de omgang met persoons- en politiegegevens raakt.

### **Artikel 10. Deskundigheid**

1. Om de taken zoals bedoeld in artikel 39 van de AVG goed uit te kunnen voeren heeft de FG kennis van onder meer:

- a. nationale en Europese wet- en regelgeving voor gegevensbescherming, zoals de AVG en de Wpg;
  - b. de gegevensverwerkingen die de organisatie uitvoert;
  - c. IT en informatiebeveiliging;
  - d. de organisatie en de sector waarin de FG actief is;
  - e. kennis van risicomanagement;
2. Daarnaast beschikt de FG over vaardigheden om binnen de organisatie een cultuur van gegevensbescherming te ontwikkelen.
  3. De FG houdt de kennis op peil via permanente educatie, trainingen en het volgen van actuele ontwikkelingen en jurisprudentie op het gebied van gegevensbescherming;
  4. De FG confirmeert zich aan de kwaliteitseisen – en normen zoals vastgesteld door het NRRFG.

#### **Artikel 11. Inwerkingtreding**

1. Dit reglement kan worden aangehaald als Reglement Functionaris voor gegevensbescherming Helmond 2025.  
[Artikel 11 lid 1 bevat een kennelijke verschrijving, hier wordt bedoeld: Dit reglement kan worden aangehaald als Reglement Functionaris voor gegevensbescherming Helmond 2026.]
2. Dit reglement treedt in werking één dag na de vaststelling en bekendmaking van dit reglement.

*Aldus besloten in de vergadering van 24 februari 2026,*

*De burgemeester,*

*De secretaris*

*De burgemeester,*