

## Reglement Functionaris Gegevens-bescherming Gemeente Enschede

### INTRODUCTIE

De Algemene Verordening Gegevensbescherming (AVG) die per 25 mei 2018 de Wet bescherming persoonsgegevens (Wbp) vervangt, geeft regels en verplichtingen ten aanzien van het verwerken van persoonsgegevens. Een van deze verplichtingen is dat overheidsinstanties, waaronder gemeenten, verplicht zijn om een Functionaris voor de gegevensbescherming (FG) aan te stellen. De belangrijkste taak van de FG is dat deze onafhankelijk toezicht en controle houdt op de toepassing en naleving van de Algemene verordening gegevensbescherming en de Wet politiegegevens.

De wet verbindt duidelijke eisen aan de positionering van een FG. Zo is het essentieel dat de FG onafhankelijk kan toezien op de naleving van de AVG in de betreffende organisatie. Naast de wettelijke bepalingen heeft de Autoriteit Persoonsgegevens (AP) ook concrete uitgangspunten opgesteld over onder meer de informatiepositie van de FG, de middelen die de FG nodig heeft en de toegang van de FG tot het bestuur van de organisatie.

In dit reglement is de landelijke regelgeving vertaald naar de gemeentelijke organisatie geeft de kaders weer voor de wijze waarop de FG van de gemeente de taken en bevoegdheden onafhankelijk en zonder enige belemmering kan uitoefenen.

De bepalingen, verplichtingen en bevoegdheden die in dit reglement worden benoemd zijn gebaseerd op de in de Algemene Verordening Gegevensbescherming gestelde eisen en op grond van de in artikel 37 AVG opgenomen verplichting voor overheidsinstanties om per 25 mei 2018 (inwerkingtreding AVG) een FG aan te stellen. De gemeente Enschede heeft sinds 2016 een FG aangesteld.

De verantwoordelijke voor de verwerking van persoonsgegevens, het College respectievelijk burgemeester, en/of het betreffende gemeentelijke bestuursorgaan, zorgt ervoor dat de onafhankelijke positie van de FG is gewaarborgd. Zodoende stelt de verantwoordelijke de FG in de gelegenheid zijn/haar taak zelfstandig, onafhankelijk en naar behoren uit te kunnen oefenen.

### POSITIE FG

De FG is een interne onafhankelijke en toezichthoudende privacyfunctionaris. De organisatie is verantwoordelijk voor het opstellen en uitvoeren van het privacy beleid. De FG ziet toe op de naleving hiervan en brengt advies uit over de risico's van bestaande verwerkingen en voorgenomen nieuwe producten en diensten. Als toezichthouder controleert de FG of de organisatie de AVG goed toepast en ziet erop toe dat betrokkenen hun privacy rechten kunnen uitoefenen. Problemen met compliance bespreekt de FG met de verantwoordelijke binnen de organisatie.

Om de onafhankelijkheid van deze functionaris te borgen zijn er uitgangspunten geformuleerd die hieraan bijdragen, waaronder:

- de FG wordt niet inhoudelijk aangestuurd en ontvangt geen instructies met betrekking tot zijn of haar taken zodat deze onafhankelijk kunnen worden vervuld (art 38, lid 3 en art 30 AVG);
- de FG ondervindt geen nadeel van de uitoefening van de rol (In artikel 38, lid 3, wordt bepaald dat functionarissen voor gegevensbescherming "door de verwerkingsverantwoordelijke of de verwerker niet ontslagen of gestraft worden voor de uitvoering van hun taken");
- de FG wordt vroegtijdig betrokken bij ontwikkelingen betreffende alle zaken die verband houden met de bescherming van persoonsgegevens (art 38 AVG). Hierbij is het belangrijk dat de organisatie er voor zorgt dat:
  - de FG regelmatig wordt uitgenodigd om vergaderingen van het hogere management en het middenkader bij te wonen en tenminste wanneer beslissingen worden genomen die gevolgen hebben voor de gegevensbescherming;
  - de FG vooraf alle relevantie informatie ontvangt over voorgenomen aanpassingen in de gegevensbescherming, zodat de FG een passend advies kan geven;
  - de mening van de FG naar behoren in overweging wordt genomen waarbij, in geval van onenigheid, het niet volgen van het advies van de FG onderbouwd wordt gedocumenteerd (conform WP29).

- de FG meteen wordt geconsulteerd zodra zich een gegevensinbreuk of ander incident voordoet.
- de FG is zichtbaar in de organisatie en is direct, zonder tussenkomst van anderen, benaderbaar en aanspreekbaar;
- de FG grijpt in als het (mogelijk) fout gaat en hij of zij risico's signaleert bij (voorgenomen) verwerkingen. De FG spreekt de organisatie hierop aan en moet op het hoogste bestuurlijke niveau zijn zorgen kunnen uiten. De organisatie moet dat faciliteren;
- de FG neemt een centrale positie in bij contacten tussen de AP en de organisatie. In die positie moet de FG op de hoogte zijn van de communicatie van de AP met de organisatie. Maar let op: de FG heeft een onafhankelijke positie en kan dus niet namens de organisatie spreken:
  - wanneer de AP contact heeft met de organisatie wordt de FG (direct of zo snel mogelijk erna) hiervan op de hoogte gesteld. Het is de verantwoordelijkheid van de organisatie om de FG tijdig en naar behoren te informeren;
  - de AP gaat ervan uit dat betrokkenen (inwoner, klanten, medewerkers) die er met de organisatie niet uitkomen, zich eerst tot de FG wenden voordat zij zich bij de AP melden. Het is niet verboden voor de betrokkene om zich direct bij de AP te melden, maar de AP wijst wel actief op de gewenste volgorde;
  - besluit de AP een formeel onderzoek te starten, dan spreekt de AP vanaf dat moment niet met de FG over de inhoud van het onderzoek. Deze duidelijkheid is niet alleen in het belang van het onderzoek, maar beschermt ook de FG. Het moet duidelijk zijn dat in deze fase de FG geen enkele inhoudelijke betrokkenheid heeft;
  - gebruik inzichten FG door AP: De AP kan adviezen van de FG aan de organisatie bij beeld- en oordeelsvorming betrekken;
  - het is voor de FG niet gepast om in een juridische procedure namens de organisatie te spreken, omdat dit zijn of haar onafhankelijke positie aantast. De organisatie kan wel voor het reguliere contact met de AP verzoeken om de FG als primair aanspreekpunt (informatieknooppunt) te laten fungeren. Afhankelijk van de fase en aard van het contact kan de AP dit toestaan.
- De FG heeft toegang tot alle (fysieke en digitale) locaties waar persoonsgegevens worden verwerkt.

Organisatorisch is de FG ondergebracht bij de Concernstaf. De FG rapporteert rechtstreeks aan de Gemeentesecretaris over zijn/haar bevindingen.

## TAKEN EN VERANTWOORDELIJKHEDEN

Het is van groot belang dat de FG zijn taken en bevoegdheden onafhankelijk en zonder enige belemmering kan uitoefenen. Deze verplichting valt onder de verantwoordelijke, het College, de burgemeester of gemeentelijke organisatie. Zij dient er ook op toe te zien dat de FG geen instructies ontvangt met betrekking tot de uitvoering van de taken. De FG heeft een belangrijke adviserende rol ten aanzien van de borging van de AVG. Vanuit een onafhankelijke positie houdt de FG intern toezicht op de manier waarop door de organisatie wordt omgegaan met persoonsgegevens.

Belangrijk is ook dat deze aan de voorkant een rol speelt bij de inrichting van processen door (gevraagd en ongevraagd) adviezen te geven ten aanzien van 'privacy by design' en 'privacy by default'.

De FG is het formele aanspreekpunt voor inwoners als zij hun rechten als betrokkene willen uitoefenen.

### DE TAKEN VAN DE FG :

- a. Het informeren en adviseren van de gemeente en de medewerkers die namens de gemeente persoonsgegevens verwerken ten behoeve van hun verplichtingen uit hoofde van de AVG/Wpb en andere Europese wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming;
- b. Het toezicht houden op de naleving van deze wet- en regelgeving bij de verwerking en bescherming van persoonsgegevens door de gemeente, en houdt toezicht op het gemeentelijk privacy- en beveiligingsbeleid en de naleving hiervan door middel van advisering en controles (art 39, lid 1, b);
- c. Gevraagd en ongevraagd adviseren en informeren van de verwerkingsverantwoordelijke en de verwerkers die namens de gemeente persoonsgegevens verwerken over onder andere:
  - hun verplichtingen aangaande de Algemene Verordening Gegevensbescherming;
  - hun verplichtingen aangaande de Wet politiegegevens
  - andere Europese wet- en regeling en nationale bepalingen omtrent gegevensbescherming;
  - overige onderwerpen die de privacy betreffen.

- d. Desgevraagd begeleiden van de werkprocessen in geval van datalekken en het toezien op het beheer van en datalekkenregister. Daarnaast heeft de FG ook de bevoegdheid om indien noodzakelijk zelf een datalek te melden bij de Autoriteit Persoonsgegevens;
- e. Samenwerken met de toezichthoudende autoriteit en optreden als contactpunt voor de toezichthoudende autoriteit inzake met verwerking verband houdende aangelegenheden, met inbegrip van het in artikel 36 bedoelde voorafgaande raadpleging en waar passend verleg plagen over enig andere aangelegenheid (art 39, lid 1, d en e). De FG fungeert als contactpunt voor zowel de Autoriteit Persoonsgegevens de interne organisatie als externe organisaties;
- f. Indien een betrokkene zijn rechten op grond van de Algemene Verordening Gegevensbescherming wil uitoefenen of een klacht heeft ten aanzien van de verwerking van persoonsgegevens, dan wordt de FG betrokken om te adviseren over het proces van besluitvorming ten aanzien van de uitoefening van deze rechten, en desgewenst een onafhankelijke bemiddelende rol spelen in de oplossing van de klacht;
- g. toezien dat verantwoordelijkheden zijn toegewezen en dat de organisatie voldoet aan de verantwoordingsplicht inzake bewustmaking en opleiding van bij de verwerking betrokken medewerkers en het uitvoeren van audits;
- h. De organisatie betreft de FG tijdig bij ontwikkelingen op het gebied van techniek en wetgeving die relevant zijn voor het gemeentelijk privacy- en beveiligingsbeleid zodat de FG de betreffende gemeentelijke diensten hierin gevraagd en ongevraagd kan adviseren.
- i. Het geven van een bindend advies met betrekking tot de Gegevensbeschermingseffectbeoordeling ofwel de Data Protection Impact Assessment (DPIA) en het toezien of de uitvoering daarvan in overeenstemming is met de Algemene Verordening Gegevensbescherming (art 39, lid 1);
- j. Uitoefening van de taak van FG als bedoeld in de wet Politiegegevens (WPG).

## TOEZICHT EN ONDERZOEK

Vanuit zijn/haar onafhankelijke toezichthoudende rol beschikt de FG over alle bevoegdheden die hem/haar in staat stellen om taken naar behoren uit te kunnen oefenen. De FG kan hierbij over bevoegdheden beschikken die gelijkwaardig zijn aan de bevoegdheden zoals geregeld in titel 5.2 van de Algemene wet bestuursrecht (Awb hoofdstuk 5 – 5.2).

In geval van twijfel of verschil van mening is het advies van de FG zwaarwegend waar alleen gemotiveerd van afgeweken kan worden. Deze motivatie wordt gedocumenteerd.

De verwerkingsverantwoordelijke (en eventuele verwerkers die bij de verwerking van persoonsgegevens zijn betrokken) verstrekken desgevraagd de FG alle inlichtingen en verlenen alle medewerking die hij/zij voor de uitoefening van zijn taak behoeft. Hiervoor heeft de FG toegang tot alle ruimten, waar een verwerking van persoonsgegevens plaatsvindt. Daarnaast is de FG bevoegd apparatuur, programmatuur, gegevensbestanden, boeken en bescheiden te onderzoeken en 'en kan daarbij, indien nodig, rekenen op hulp ten aanzien van de werking van apparatuur en programmatuur'.

Indien noodzakelijk krijgt de FG toegang tot de (computer-)systemen waarin persoonsgegevens worden verwerkt. De FG zal desnoods de beschikking dienen te krijgen over de relevante inloggegevens. De FG wordt in staat gesteld om zaken daadwerkelijk te onderzoeken.

De FG dient zelfstandig en onafhankelijk over zijn/haar bevindingen aan de verwerkingsverantwoordelijke te rapporteren. De FG adviseert over te nemen maatregelen (zowel regressief als progressief) om risico's te beperken of weg te nemen. Verder kan de FG een onderzoek instellen naar de wijze waarop in verband met de verwerking van persoonsgegevens, in een bepaald geval dan wel in het algemeen belang, de persoonlijke levenssfeer wordt beschermd.

Indien de FG dit naar redelijkheid nodig acht, kan de FG voor zijn/haar onderzoek gebruikmaken van de diensten van externe specialisten.

## REGISTERS

### A. REGISTER GEGEVENSVERWERKINGEN

De verwerkingsverantwoordelijke houdt een register bij van de verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden (art 30, lid 1 en 2). De Functionaris Gegevensbescherming ziet er op toe dat een dergelijk register wordt bijgehouden en adviseert de verwerkingsverantwoordelijke en/of de verwerker over de inhoud, actualiteit en compleetheid hiervan.

## B. DATALEKKEN REGISTER

De organisatie heeft een meldprocedure en een datalekkenregister. In het register worden alle datalekken geregistreerd, zowel de datalekken die worden gemeld bij de Autoriteit Persoonsgegevens als de datalekken die niet extern worden gemeld.

Indien het verlies of misbruik van persoonsgegevens betreft dat ernstig nadelige gevolgen voor de betrokkene kan hebben/heeft, wordt de betrokkene ook ingelicht. Datalekken worden in het datalekregister genoteerd.

De Functionaris Gegevensbescherming ziet er op toe dat een dergelijk register wordt bijgehouden en adviseert de verwerkingsverantwoordelijke of de verwerker over de inhoud, actualiteit en compleetheid hiervan.

In het datalekregister wordt informatie over onderstaande onderwerpen vastgelegd:

- een omschrijving van het datalek;
- de datum van het datalek;
- de duur van het datalek;
- het soort persoonsgegevens dat is gelekt;
- het aantal betrokkenen;
- het aantal ontvangers;
- eventuele betrokkenheid van derde partijen;
- oorzaak datalek;
- verantwoordelijk organisatieonderdeel;
- de aard van de inbreuk (bijvoorbeeld: een inbreuk of de vertrouwelijkheid beschikbaarheid en de integriteit);
- een beschrijving van de gevolgen van het datalek;
- de genomen maatregelen;
- is de FG betrokken en zo ja, in welke mate;
- wel of niet gemeld aan betrokkenen (met motivatie);
- wel of niet gemeld bij de AP (met motivatie).

## BENODIGDE MIDDELEN

De verwerkingsverantwoordelijke stelt aan de FG het benodigde werkbudget ter beschikking om aan diens taken en verplichtingen te voldoen.

Krachtens artikel 38, lid 2, van de algemene verordening gegevensbescherming moet de organisatie haar Functionaris voor Gegevensbescherming ondersteunen door "hem toegang te verschaffen tot persoonsgegevens en verwerkingsactiviteiten en door hem de benodigde middelen ter beschikking te stellen voor het vervullen van zijn/haar taken en het in stand houden van zijn deskundigheid". Met name de volgende items moeten in aanmerking worden genomen:

- actieve ondersteuning door het hogere management;
- voldoende tijd om de taken te vervullen;
- adequate ondersteuning op het vlak van financiële middelen, infrastructuur en personele ondersteuning waar van toepassing;
- noodzakelijke toegang tot andere afdelingen (HR, juridische zaken, IT, beveiliging etc.) om de nodige ondersteuning, bijstand of informatie te kunnen ontvangen;
- opleiding zodat de FG de kans krijgt om op de hoogte te blijven van nieuwe ontwikkelingen op het vlak van gegevensbescherming. Daarbij moet het de bedoeling zijn het niveau van de deskundigheid van FG permanent te verhogen door deze in staat te stellen om deel te nemen aan opleidingen over gegevensbescherming en aan andere vormen van professionele ontplooiing, zoals deelname aan fora over privacy, workshops enz.;
- duidelijk vastleggen van de interne structuur van het team dat de FG ondersteunt bij zijn/haar taken, waarbij de taken en verantwoordelijkheden van een ieder duidelijk worden vastgelegd.