**Handreiking FG mbo**

**(versie 1.0, mei 2019)**

**IBPDOC34**

Verantwoording

**Bron:**

**Handreiking FG po/vo (versie 1.2)**

*PO-Raad, VO-raad en Kennisnet*

*April 2018*

**Bewerkt door:**

Kennisnet / saMBO-ICT / MBO Raad

**Auteurs**

Leo Bakker (Kennisnet)

Niels Dutij (Functionaris voor gegevensbescherming bij meerdere mbo-instellingen)

Debby Sikking (Kennisnet)

Peter Vermeijs (MBO Raad)

Job Vos (Kennisnet)

*Mei 2019*

**Met dank aan**

Wim Arendse (Regiegroep IBP mbo; Zadkine)

**Sommige rechten voorbehouden**

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(s) en uitgevers geen aansprakelijkheid voor eventuele fouten, onvolkomenheden of schade als gevolg van het gebruik van dit document. Bij twijfel of juridische geschillen wordt geadviseerd om een deskundige in te huren zoals een advocaat, ict-consultant of een in privacy gespecialiseerd jurist.

**Creative commons**

Naamsvermelding 3.0 Nederland

(CC BY 3.0)

**De gebruiker mag:**

* Het werk kopiëren, verspreiden en doorgeven
* Remixen – afgeleide werken maken

**Onder de volgende voorwaarde:**

* Naamsvermelding – De gebruiker dient bij het werk de naam van Kennisnet te vermelden (maar niet zodanig dat de indruk gewekt wordt dat zij daarmee instemt met uw werk of uw gebruik van het werk).

***Waar in deze publicatie geschreven wordt in de mannelijke vorm, kan mede de vrouwelijk vorm gelezen worden.***

**Inhoud**

[**Verantwoording 2**](#_Toc9256545)

[**Managementsamenvatting 5**](#_Toc9256546)

[**1. Inleiding 6**](#_Toc9256547)

[**2. Wettelijk kader aanstellen FG 7**](#_Toc9256548)

[**2.1. Belangrijke begrippen over privacy 7**](#_Toc9256549)

[**2.2. Wie bepaalt of een FG aangewezen moet worden? 8**](#_Toc9256550)

[**2.3. Autoriteit Persoonsgegevens 8**](#_Toc9256551)

[**2.4. Moet volgens de wet een FG aangewezen worden? 8**](#_Toc9256552)

[**2.5. Wat als er tijdelijk geen FG is aangewezen? 9**](#_Toc9256553)

[**3. Aanwijzen FG 10**](#_Toc9256554)

[**3.1. Aanwijzen FG 10**](#_Toc9256555)

[**3.2. Functie 10**](#_Toc9256556)

[**3.3. Positionering en combineren functies 11**](#_Toc9256557)

[**3.4. Medezeggenschap 11**](#_Toc9256558)

[**3.4.1. Medezeggenschap medewerkers 11**](#_Toc9256559)

[**3.4.2. Medezeggenschap studenten 11**](#_Toc9256560)

[**3.4.3. Medezeggenschap ouders 12**](#_Toc9256561)

[**3.5. Autoriteit Persoonsgegevens 12**](#_Toc9256562)

[**3.5.1. Aanmelding FG 12**](#_Toc9256563)

[**3.6. Privacy Officer 12**](#_Toc9256564)

[**3.7. Interne of externe FG 13**](#_Toc9256565)

[**3.8. Samenwerking tussen besturen 13**](#_Toc9256566)

[**3.9. Bekend maken aanwijzen FG 14**](#_Toc9256567)

[**3.10. Aansprakelijkheid 14**](#_Toc9256568)

[**4. Taken en bevoegdheden FG 15**](#_Toc9256569)

[**4.1. Taken FG 15**](#_Toc9256570)

[**4.2. Uitvoering taken 15**](#_Toc9256571)

[**4.3. Bevoegdheden 16**](#_Toc9256572)

[**5. Expertise, functie-eisen en rechtspositie FG 17**](#_Toc9256573)

[**5.1. FG als professional 17**](#_Toc9256574)

[**5.2. Vereiste expertise en vaardigheden 17**](#_Toc9256575)

[**5.3. Onafhankelijkheid 17**](#_Toc9256576)

[**5.4. Ontslagbescherming 17**](#_Toc9256577)

[**Bijlage 1: Juridische onderbouwing aanwijzen FG 19**](#_Toc9256578)

[**1.1. Artikel 37 AVG 19**](#_Toc9256580)

[**1.2. De mbo-instelling als overheidsinstantie of overheidsorgaan 20**](#_Toc9256581)

[**1.3. Hoofdzakelijk belast met regelmatige en stelselmatige observatie op grote schaal 21**](#_Toc9256582)

[**1.3.1. Hoofdzakelijk belast: kerntaken 21**](#_Toc9256583)

[**1.3.2. Op grote schaal 22**](#_Toc9256584)

[**1.3.3. Regelmatige en stelselmatige observatie 23**](#_Toc9256585)

[**1.3.4. Aard, omvang en/of doeleinden van de verwerking van persoonsgegevens 23**](#_Toc9256586)

[**1.4. Grootschalige verwerking van bijzondere categorieën persoonsgegevens en/of strafrechtelijke veroordelingen en strafbare feiten 23**](#_Toc9256587)

[**1.5. Moet volgens de wet een FG aangewezen worden? 24**](#_Toc9256588)

[**1.6. Uitzondering: geen FG aanwijzen 24**](#_Toc9256589)

[**Bijlage 2: Regeling taken en bevoegdheden FG 26**](#_Toc9256590)

[**Bijlage 3: voorbeeld vacaturetekst FG 28**](#_Toc9256591)

**Managementsamenvatting**

Onderwijsinstellingen maken steeds beter en meer gebruik van ict. Daardoor neemt het aantal persoonsgegevens dat wordt gebruikt, toe. Het beschermen van de privacy van studenten en medewerkers wordt daarom steeds belangrijker. Colleges van Bestuur van een mbo-instelling zijn volgens de wet verplicht om privacy goed te regelen.

Op 25 mei 2018 is de Europese Algemene Verordening Gegevensbescherming (AVG) in werking getreden die op een aantal punten strenger is dan de Nederlandse Wet bescherming Persoonsgegevens. Privacy moet volgens deze AVG een belangrijke plaats krijgen en houden in organisaties. Een van de belangrijke wijzigingen is dat organisaties verplicht worden om in een aantal gevallen een functionaris voor gegevensbescherming (FG) aan te stellen. Naast het aanwijzen van een FG zijn er meerdere zaken die een College van Bestuur moet regelen. In het [Framework ibp in het mbo](https://www.sambo-ict.nl/netwerken/informatiebeveiliging/framework-ibp/) 2.0 is een overzicht opgenomen wat mbo-instellingen nog meer moeten regelen en waar mbo-instellingen mee kunnen beginnen om informatiebeveiliging en privacy te regelen.

Een FG is een interne toezichthouder op de verwerking van persoonsgegevens binnen een organisatie. Deze functionaris heeft geen formele sanctiebevoegdheden, maar wel controlebevoegdheden. Hij adviseert het College van Bestuur (bevoegd gezag) over privacy en houdt toezicht daarop, handelt vragen en klachten over privacy af, ontwikkelt (interne) regelingen rondom privacy en geeft advies over technologie en beveiliging (privacy by design). De FG moet voldoende kennis hebben van de organisatie en van privacywetgeving, betrouwbaar zijn en moet in onafhankelijkheid zijn werkzaamheden kunnen verrichten. De FG heeft dezelfde ontslagbescherming als leden van de ondernemingsraad (OR).

Uit juridische analyse van de AVG blijkt dat Colleges van Bestuur verplicht zijn om een FG “aan te wijzen”. De MBO Raad, saMBO-ICT en Kennisnet bevelen Colleges van Bestuur (bevoegd gezag) aan om een FG aan te wijzen. Ieder College van Bestuur heeft een FG nodig (dus niet per vestiging of locatie). De aangewezen FG moet worden aangemeld bij de toezichthouder voor privacy in Nederland: de Autoriteit Persoonsgegevens.

Het is mogelijk om intern een medewerker als FG aan te wijzen, of om een externe FG in te huren. De AVG geeft de mogelijkheid dat Colleges van Bestuur samen een (interne of externe) FG aanwijzen. Voorwaarde daarbij is dat de FG wel de organisaties van de Colleges van Bestuur kent waarvoor hij werkzaam is en weet wat er speelt, op tijd geraadpleegd wordt bij besluiten over privacy en op de hoogte is van wat er geregeld is rondom de privacy van studenten en medewerkers binnen het College van Bestuur. Daarnaast moet de FG onafhankelijk zijn zodat er geen belangenconflict mag ontstaan bij de uitvoering van diens taken.

De FG bemoeit zich binnen de instelling met de privacy van medewerkers en studenten. Daarom is voorafgaand aan het aanwijzen van een FG, de instemming van de OR, studentenraad en – indien van toepassing – de ouderraad noodzakelijk. Daarbij gaat het niet om de *persoon* van de FG maar om diens taken, rechten en bevoegdheden en het vaststellen van het reglement voor de FG.

In deze Handreiking wordt uitgelegd op welke grond een College van Bestuur een FG moet aanwijzen, hoe je die aanwijzing regelt, wat diens taken en bevoegdheden zijn en wat de functie-eisen zijn. Daarnaast wordt in de bijlagen een juridische onderbouwing gegeven waarom een FG vereist is, en zijn een voorbeeld-reglement voor de FG en voorbeeld-functieomschrijving opgenomen.

1. **Inleiding**

In Nederland wordt privacy sinds 25 mei 2018 beschermd door de in heel Europa geldende Algemene de *Algemene Verordening Gegevensbescherming (AVG)*. Deze Europese wet is direct van toepassing is in alle landen van de Europese Unie. In het Engels wordt de AVG General Data Protection Regulation (GDPR) genoemd. Deze AVG is strenger dan de oude Wet bescherming persoonsgegevens (Wbp). Zo worden de rechten van de personen over wiens privacy het gaat, versterkt en uitgebreid. Ook krijgen organisaties die persoonsgegevens gebruiken, meer verantwoordelijkheden en verplichtingen. Organisaties moeten bijvoorbeeld voortaan aantoonbaar voldoen aan de AVG, zij moeten dus kunnen laten zien dat ze de wet naleven. Er wordt ook meer samengewerkt tussen alle Europese privacy-toezichthouders. Daarnaast zijn de boetes die ze kunnen opleggen verhoogd ~~zijn~~ naar 20 miljoen euro, of zelfs 4% van de jaaromzet van een onderneming.

Een andere belangrijke wijziging is dat organisaties intern hun privacy(beleid) beter moeten organiseren. Privacy moet een belangrijke en permanente plaats krijgen en houden in organisaties. Een maatregel om dat te bereiken, is volgens de AVG het aanwijzen van een interne privacy-toezichthouder. Die persoon wordt *functionaris voor gegevensbescherming* (afgekort: *FG*) genoemd. In het Engels wordt de FG *Data Protection officer (DPO)* genoemd.

De verplichting om een FG aan te stellen, geldt ook voor Colleges van Bestuur. In deze handreiking wordt uitgelegd dat het aanwijzen van een FG voor Colleges van Bestuur verplicht is, hoe je dat regelt, wat diens taken en bevoegdheden zijn, wat een mogelijke vacaturetekst kan zijn, en hoe te handelen als je (tijdelijk/nog) geen FG hebt aangewezen. **Uit analyse van de tekst van de AVG die in deze handreiking is opgenomen, volgt dat het aanwijzen van een FG door het College van Bestuur verplicht is.**

***Framework ibp in het mbo 2.0***

Onderwijsinstellingen in het po, vo en mbo zijn op bestuursniveau verplicht om informatiebeveiliging en privacy (afgekort tot **IBP**) voor hun organisatie te regelen. Het aanstellen van een FG is daar een onderdeel van. Wil een mbo-instelling met ict persoonlijk, eigentijds en veilig onderwijs geven, dan moet IBP goed geregeld zijn.

Het regelen van een FG is slechts één van de (vele) zaken die een mbo-instelling moet regelen in verband met de invoering van de AVG. Om onderwijsinstellingen te helpen zijn verschillende hulpmiddelen ontwikkeld die onderwijsinstellingen helpen op een eenvoudige én gestructureerde wijze IBP te implementeren. In het mbo is er het ‘**Framework ibp in het mbo 2.0**’[[1]](#footnote-2), voor het po en vo is de '**Aanpak IBP po/vo**'**[[2]](#footnote-3)** ontwikkeld,

Het Framework ibp in het mbo en de Aanpak IBP zijn gebaseerd op de AVG, maar ook op de internationale standaard voor informatiebeveiliging, de ISO 27001 en 27002. Deze wet- en regelgeving is vertaald naar praktische en begrijpelijke maatregelen, beleid en voorbeelddocumentatie.

1. **Wettelijk kader aanstellen FG**

*In dit hoofdstuk worden de basisprincipes van privacy beschreven, en wordt uitgelegd dat het College van Bestuur een FG moeten aanwijzen.*

* 1. **Belangrijke begrippen over privacy**

Voor een goed begrip van privacy, is het noodzakelijk de basisbegrippen van privacy te kennen.

Privacywetgeving gaat over persoonsgegevens. Dat zijn alle gegevens waarmee direct of indirect een natuurlijk

persoon (mens) kan worden geïdentificeerd. Het kan bijvoorbeeld gaan om een naam, BSN-nummer,

geboortedatum, telefoonnummer of IP-adres. Studentgegevens zijn dan ook persoonsgegevens. Gevoelige informatie over studenten en medewerkers, zoals informatie over gezondheid, gedragsproblemen, politieke voorkeur, godsdienst, seksuele voorkeur of een problematische thuissituatie noemen we bijzondere persoonsgegevens. In de AVG vallen genetische gegevens en biometrische gegevens ook onder de categorie bijzondere persoonsgegevens. Bijzondere persoonsgegevens mogen niet worden gebruikt, tenzij de wet of de betrokkene daar expliciet toestemming voor geeft.

Alles wat met persoonsgegevens wordt gedaan, wordt in de wet verwerken genoemd. Verwerken is dus onder meer: online en offline persoonsgegevens verzamelen, kopiëren, opslaan, verspreiden, publiceren, delen én uitwisselen. Het maakt dus niet uit wat je doet met persoonsgegevens: al het gebruik van persoonsgegevens noemen we verwerken. Kort door de bocht kun je stellen dat het 'aanraken' van persoonsgegevens al verwerken is, waardoor de AVG van toepassing is.

De verwerkingsverantwoordelijke is een natuurlijk persoon of instantie die vaststelt welke persoonsgegevens er verwerkt worden én wat het doel is van die verwerking. Het gaat hier om de persoon of instantie die formeel en juridisch het initiatief neemt tot het verzamelen van persoonsgegevens en daarvoor ook verantwoordelijk is. In het mbo is dit het bestuur van de rechtspersoon waar de mbo-instelling onder valt: het College van Bestuur of bevoegd gezag. Gemakshalve spreken we in deze handreiking over ‘de mbo-instelling’, maar we bedoelen dan eigenlijk het College van Bestuur.

De verwerker verwerkt de persoonsgegevens namens de verwerkingsverantwoordelijke. Een voorbeeld is een mbo-instelling die voor het vastleggen van de studievoortgang van studenten een studentinformatiesysteem gebruikt. Deze leverancier is dan verwerker voor de mbo-instelling. De verwerker handelt in opdracht van de verwerkingsverantwoordelijke en mag alleen verwerkingen doen waarvoor hij uitdrukkelijk opdracht krijgt. De verwerker neemt dus geen zelfstandige beslissing over de gegevens, dat is formeel het College van Bestuur. Er is geen hiërarchische verhouding tussen de verwerkingsverantwoordelijke en de verwerker: een verwerker is dus nooit in loondienst bij de verwerkingsverantwoordelijke.

De betrokkene is de mens over wie de persoonsgegevens gaan: de student. Maar het kan ook gaan over een medewerker van de mbo-instelling zoals de conciërge, decaan, opleidingsmanager, docent of de directeur. Als de betrokken student jonger is dan 16 jaar, dan mogen volgens de wet alleen zijn wettelijke vertegenwoordigers (ouders) beslissen over de gegevens van de betrokkene, de student/student beslist dus dan niet zelf over zijn privacy.

Een functionaris voor gegevensbescherming (FG) is een persoon met deskundige kennis van gegevensbeschermingswetgeving en -praktijken die binnen de organisatie toezicht houdt op de toepassing en naleving van privacywet- en regelgeving. De FG is tijdig en adequaat betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens binnen de organisatie waar de FG is aangesteld. De FG kan een aanspreekpunt zijn voor de betrokkenen bij uitoefening van hun rechten tegenover de verwerkingsverantwoordelijke of verwerker. Ook kan de FG fungeren als tussenpersoon of vertegenwoordiger bij (afspraken over) verwerkingen van persoonsgegevens met of tussen verschillende organisaties.

Het toezicht op privacy en op de toepassing van de AVG, wordt in Nederland uitgeoefend door de Autoriteit Persoonsgegevens (afgekort tot AP).

* 1. **Wie bepaalt of een FG aangewezen moet worden?**

Of een organisatie een FG moet aanwijzen, staat in de AVG. In eerdere teksten van de AVG (2015) was opgenomen dat een organisatie een bepaalde grootte moest hebben (bijvoorbeeld 250 werknemers of 5000 betrokkenen). In 2016 is bewust gekozen om dit criterium uit de AVG te schrappen: het maakt dus niet (meer) uit of het een kleine of grote organisatie betreft. Het gaat om de aard en omvang van de persoonsgegevens die worden verwerkt.

In de onderhandelingen tussen de Europese Commissie, Europees Parlement en de Raad van Ministers is gediscussieerd over de verplichting om een FG aan te wijzen. De bedoeling van het aanwijzen van een FG is om meer toezicht en controle op de verwerking van persoonsgegevens te creëren. Mede daarom is overwogen dat de grootte van een organisatie wellicht geen goed criterium is. Een doorsnee bedrijf met 1000 werknemers kan minder ‘gevoelige’ persoonsgegevens verwerken dan een marketingbureau met 25 medewerkers. Daarmee is een functioneel criterium geïntroduceerd wanneer een FG verplicht is (zie toelichting in paragraaf 2.4).

Omdat concrete criteria ontbreken, moet een organisatie zelf aan de hand van de AVG bepalen of een FG voor hen verplicht is. Achteraf kan getoetst worden door de toezichthouder of een FG aangewezen had moeten worden. In paragraaf 2.4 is de juridische onderbouwing gegeven. Deze handreiking helpt Colleges van Bestuur *zelf* te beslissen of zij vallen onder de criteria van de AVG om een FG aan te wijzen.

De verwerkingsverantwoordelijke is eindverantwoordelijk voor privacy binnen een organisatie. Onder die verantwoordelijkheid valt ook het aanstellen van een FG. Concreet voor het onderwijs betekent dit dat Colleges van Bestuur van een mbo-instelling formeel de keuze moeten maken een FG aan te wijzen. Hiervoor is een gemotiveerd bestuursbesluit nodig. Na dat besluit moet de FG zich aanmelden bij de AP (zie paragraaf 3.5.1) voordat de FG officieel in functie is.

* 1. **Autoriteit Persoonsgegevens**

Gezien de vrijheid van onderwijs zoals die in de Grondwet is geregeld, neemt het onderwijs in Nederland een redelijk unieke positie in ten opzichte van mbo-instellingen in omliggende Europese landen. Onderwijs is in Europa doorgaans meer georganiseerd door overheden of vanuit overheidswege, waardoor onderwijsinstellingen sneller gezien worden als overheidsinstanties zodat daaruit een verplichting om een FG aan te wijzen voor de hand ligt (art. 37 lid 1 sub a AVG). Alhoewel dat praktisch zou zijn, mag de AP niet ‘zelfstandig’ vaststellen voor het onderwijs in Nederland dat een FG verplicht is op basis van de AVG. De AP moet dat afstemmen in Europees verband. Zou de AP een dergelijke uitspraak wel doen, dan zou dat betekenen dat mbo-instellingen in heel Europa ‘dus’ een FG moeten hebben. De verwachting is niet dat de AP op korte termijn hier duidelijkheid over zal verschaffen. Daarbij blijkt uit de praktijk dat alle onderwijsinstellingen in het mbo inmiddels een FG hebben aangewezen.

Het is op dit moment ook nog niet duidelijk of de AP met regels komt over het aanwijzen van een FG, of voor bijvoorbeeld opleidingseisen voor FG’s, of dat er eisen voor een gedragscode of certificering komen. Wel is de verwachting dat de AP op hoofdlijnen voorlichting zal (gaan) geven over de functie van FG onder de AVG. Op korte termijn worden er geen wijzigingen verwacht. De AVG stelt echter al wel eisen aan de kwaliteiten voor de functionaris voor gegevensbescherming, zie hiervoor hoofdstuk 5. Het is dus niet mogelijk om zomaar iemand aan te wijzen als functionaris voor gegevensbescherming.

* 1. **Moet volgens de wet een FG aangewezen worden?**

Op basis van analyse van de wetgeving (die is opgenomen als bijlage 1) is de conclusie van de sectorraden, saMBO-ICT en Kennisnet dat een College van Bestuur - vanaf 25 mei 2018 – wel een FG dient aan te wijzen op grond van de AVG, artikel 37 lid 1 sub:

1. Het College van Bestuur is niet snel aan te merken als of gelijk te stellen aan een *overheidsinstantie of overheidsorgaan*, alhoewel daar onder omstandigheden wel sprake van kan zijn;
2. Het College van Bestuur is hoofdzakelijk *belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen* vereisen.

De verplichting om een FG aan te wijzen, geldt voor een College van Bestuur (en niet per vestiging of locatie). Kortheidshalve wordt voor een verdere uitleg verwezen naar bijlage 1 waarin wordt ingegaan op de hierboven genoemde gronden. Uit deze analyse van de AVG volgt dat Colleges van Bestuur (bevoegd gezagen) een FG moeten aanwijzen.

* 1. **Wat als er tijdelijk geen FG is aangewezen?**

De AVG verplicht Colleges van Bestuur om een FG aan te wijzen. Het is mogelijk dat een mbo-instelling nog niet of tijdelijk niet over een FG beschikt (bijvoorbeeld door vertrek van de huidige FG). Voor Colleges van Bestuur die tijdelijk geen FG hebben aangewezen, maar wel bezig zijn om die te regelen, is het advies om schriftelijk vast te leggen waarom ze (tijdelijk) geen FG hebben aangewezen en wat de planning is om wel aan die verplichting te gaan voldoen. Daarmee kan het College van Bestuur verantwoorden waarom er (tijdelijk) niet de AVG wordt voldaan en wanneer verwacht wordt wel over een FG te beschikken (dit sluit aan bij het principe ‘comply of explain’).

Door dit besluit te documenteren, wordt aangesloten bij het begrip van ‘accountability’ dat uitgangspunt is in de AVG. Het kan daarbij helpen om een interne medewerker tijdelijk aan te wijzen als FG (ad interim) of om de privacy officer te vragen te fungeren als vraagbaak en te acteren bij incidenten.

1. **Aanwijzen FG**

*Dit hoofdstuk beschrijft hoe je een FG aanwijst.*

* 1. **Aanwijzen FG**

Het aanwijzen van een FG kan bij besluit van het College van Bestuur, dat schriftelijk gemotiveerd is. De AVG spreekt over het ‘aanwijzen’ van een FG en niet over het ‘aanstellen’. In de praktijk wordt ook wel gesproken over het ‘benoemen van X tot FG’.

Gelijktijdig met het aanwijzen van de FG kan een ‘Regeling voor de taken en verantwoordelijk FG’ worden vastgesteld, een voorbeeld hiervan is opgenomen in bijlage 2. Daarin wordt geregeld wat de taken en bevoegdheden van de FG zijn.

Omdat aan het aanwijzen van een FG wettelijke eisen zijn gesteld, kan de titel FG niet zomaar worden gebruikt, en er kan niet worden afgeweken van een formele aanwijzing. Iemand belast met privacy binnen de organisatie kan zich niet plotseling ‘FG’ gaan (laten) noemen. Het is een wettelijk beschermde titel. Een FG is pas aangewezen als FG als er een besluit is, en de FG is geregistreerd bij de AP als FG.

Het is goed om te voorkomen dat door het aanwijzen van een FG niet het beeld ontstaat ‘*dat er niets meer mag*’. De interne controlerende functie is slechts één van de taken van een FG (zie hoofdstuk 5 over taken en bevoegdheden). Goede communicatie over het aanwijzen van de FG is daarom erg belangrijk. Een goede FG kan een constructieve bijdrage leveren aan het organiseren en bevorderen van informatiebeveiliging en privacy binnen een College van Bestuur. Zorg dat de aangewezen FG een gesprekpartner is (wordt) voor bestuur, medewerkers maar ook voor studenten (en hun ouders).

* 1. **Functie**

In het kader van het personeelsbeleid, moet worden vastgesteld dat de FG een functie is: een vast omlijnd pakket met taken, werkzaamheden en verantwoordelijkheden die gekoppeld zijn aan een persoon. Een FG is dus geen rol (pakket van taken losgekoppeld van een persoon). De functie van FG is niet flexibel uitwisselbaar aangezien aan een aantal formele vereisten moet worden voldaan (zoals een aanwijzing door het bestuur). Vanwege dat onafhankelijk toezicht en in vrijheid kunnen opereren en adviseren, is het ook wenselijk dat de FG niet steeds wisselt. De functie van FG hoeft geen fulltime functie te zijn, het kan ook gecombineerd worden met andere werkzaamheden die een interne medewerker verricht.

Let op: naleving van regels op het gebied van gegevensbescherming is een bedrijfsverantwoordelijkheid van de verwerkingsverantwoordelijke (College van Bestuur), en niet van de FG. De FG houdt toezicht, maar is niet verantwoordelijk voor de nakoming van regels.

* 1. **Positionering en combineren functies**

Voor wat betreft de positionering van de FG binnen de organisatie, schrijft de AVG voor dat de FG onafhankelijk moet zijn (zie daarover meer in paragraaf 5.3), en rechtstreeks verslag uitbrengt aan de hoogste leidinggevende binnen de organisatie, namelijk het College van Bestuur.

De FG mag geen positie in de organisatie hebben die ertoe leidt dat hij het doel van en de middelen voor het verwerken van persoonsgegevens bepaalt. Dit maakt dat niet iedereen FG kan worden: een lid van het College van Bestuur, directeur of manager bedrijfsvoering zal geen FG kunnen worden als de FG zijn eigen werk moet gaan controleren. Maar ook een hoofd administratie (personeel of studenten) ligt minder voor de hand: die is in de dagelijkse praktijk betrokken bij de besluitvorming over persoonsgegevens en kan daarom geen onafhankelijk toezicht houden.

Het is mogelijk dat een medewerker die reeds in dienst is, wordt aangewezen als FG (en dus de functie FG krijgt). Naast de eis dat deze FG voldoet aan de in AVG opgenomen specifieke kwaliteitseisen, is voorwaarde dat deze medewerker vanuit een onafhankelijke positie de functie van FG kan uitoefenen (zie paragraaf 3.3). Het kan verstandig zijn om interne regels op te stellen om belangenconflicten te vermijden, of te bepalen welke taken de FG niet mag uitvoeren.

Het komt voor dat een instellingsjurist, compliance officer, vertrouwenspersoon of controller als FG worden aangewezen. Hoewel dit mogelijk kan zijn, dient de organisatie telkens af te wegen of er ook echt sprake blijft van onafhankelijkheid. Zo zal een jurist ook vaak beleid of reglementen opstellen, terwijl dat conflicteert met de taak van de FG als toezichthouder.

* 1. **Medezeggenschap**
		1. **Medezeggenschap medewerkers**

Volgens de Wet op de ondernemingsraden (WOR) heeft de OR instemmingsrecht in geval van vaststelling of wijziging van een regeling over het verwerken van en de bescherming van persoonsgegevens van medewerkers (artikel 27 lid 1 sub K WOR).

Aan het aanwijzen van een FG gaan keuzes vooraf over (de grootte van) het takenpakket, diens bevoegdheden, regeling voor de taken en werkzaamheden van de FG, de mogelijke contractomvang of taakuren, plaats binnen of buiten de organisatie, etc. Daarnaast heeft de FG een toezichthoudende taak en mag deze persoonsgegevens van medewerkers inzien in het kader van de controlerende functie. Deze keuzes rondom het aanwijzen van een FG maken onderdeel uit van de besluitvorming over het intern toezicht op gegevensbescherming van studenten, ouders en medewerkers. Daarop is het instemmingsrecht van de OR van toepassing.

Dit betekent dat de instemming van de OR vereist is voor het aanwijzen van een FG, en het vaststellen van het Reglement FG. Daarbij is er geen instemmingsrecht op de ‘persoon’ van de FG, maar over keuzes over de functie, inrichting en taken van de FG. De OR stemt in met het aanwijzen van een FG, niet wie de FG wordt. De OR toetst onder meer of de FG zijn functie daadwerkelijk onafhankelijk kan vervullen, of dat de FG voldoende tijd en middelen heeft om zijn werk naar behoren te verrichten en om kennis op peil te houden.

* + 1. **Medezeggenschap studenten**

Voor studenten is medezeggenschap geregeld in de Wet educatie en beroepsonderwijs (WEB). Daarin is geregeld dat er aan iedere mbo-instelling een deelnemersraad (beter bekend als studentenraad) verbonden is. Deze studentenraad heeft een instemmingsrecht met betrekking tot voorgenomen beslissingen van het College van Bestuur die betrekking hebben op “de wijze van vastleggen van studievorderingen van studenten en in dat verband het beleid met betrekking tot bescherming van de privacy van studenten” (art 8a.2.2 lid 3 onder j WEB). Een FG is ook betrokken bij de bescherming van persoonsgegevens van studenten, en de FG heeft een controlerende bevoegdheid die ook ziet op de systemen waarin de studievorderingen zijn opgenomen. Het aanwijzen van een FG en het vaststellen van het reglement van de FG heeft hier – in ieder geval – indirect mee te maken. Het verdient daarom aanbeveling om de studentenraad te betrekken bij het aanwijzen van een FG, gelijk de OR daar instemming op moet geven. Voor zover de mbo-instelling van mening is dat de studentenraad niet om instemming hoeft te worden gevraagd (of als dat niet specifiek is geregeld in het medezeggenschapsstatuut), zal dit ten minste moeten worden medegedeeld.

* + 1. **Medezeggenschap ouders**

Naast een OR en studentenraad, kan er een ouderraad worden ingesteld. De ouderraad heeft de zelfde bevoegdheden als de studentenraad (art. 8a.1.3 lid 4 WEB). Zoals in paragraaf 3.4.2 is uitgelegd, verdient het aanbeveling om de ouderraad te betrekken bij het aanwijzen van een FG, gelijk de OR daar instemming op moet geven. Voor zover de mbo-instelling van mening is dat de ouderraad niet om instemming hoeft te worden gevraagd (of als dat niet specifiek is geregeld in het medezeggenschapsstatuut), zal dit ten minste moeten worden medegedeeld.

Voor een school in het voortgezet onderwijs die zich met een regionaal opleidingencentrum verenigt tot een scholengemeenschap (scholengemeenschap ROC of AOC-school voor voortgezet onderwijs als bedoeld in artikel 2.6 WEB), geldt dat de uit en door de ouders gekozen deel van MR van die vo-school de (eerste) ouderraad van de scholengemeenschap vormt. Op deze ouderraad zijn niet de bepalingen van de Wet medezeggenschap onderwijs (po en vo) van toepassing, maar de regels voor de ouderraad zoals deze in de WEB zijn opgenomen.

* 1. **Autoriteit Persoonsgegevens**

Het is de bedoeling van de wetgever dat zich tussen de FG en de toezichthouder, de AP, een “soepel samenspel” ontwikkelt. De FG is geen verlengde arm van de Autoriteit Persoonsgegevens: hij is dan ook niet verplicht om de AP uit eigen beweging informatie te verstrekken. De FG moet gezien worden als eerste-lijnstoezichthouder en hij kan als intermediair optreden tussen het bestuur en de toezichthouder. Voorwaarde is dan wel dat er sprake is van het uitoefenen van geloofwaardig en effectief toezicht door de FG.

De AP houdt toezicht of organisaties de functie van FG naar behoren hebben ingericht, en of dat in de praktijk ook goed wordt uitgevoerd. De FG is immers een interne toezichthouder, en dat toezicht moet – met de nodige waarborgen - goed geregeld zijn.

* + 1. **Aanmelding FG**

Op basis van de AVG houdt de Autoriteit Persoonsgegevens een register bij van alle aangewezen FG’s. Een FG is verplicht om zich als FG aan te melden bij de AP. Pas dan is de aanwijzing definitief.

Er is een aanmeldingsformulier voor FG’s beschikbaar bij de Autoriteit Persoonsgegevens: <https://www.autoriteitpersoonsgegevens.nl/nl/aanmeldingsformulier-functionaris-voor-de-gegevensbescherming-fg>

LET OP: FG-aanmeldingen die *niet* via het online aanmeldingsformulier zijn gedaan (dus voor mei 2018), zijn komen te vervallen.

Meer informatie van de AP over de FG en aanmelding, kan je hier vinden: <https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/functionaris-gegevensbescherming-fg?qa=fg>.

* 1. **Privacy Officer**

Het komt voor dat een organisatie wel iemand heeft aangesteld of aangewezen met privacy als aandachtsgebied, zoals bijvoorbeeld een privacy officer (po) of een juridisch adviseur privacy, maar (nog) geen FG heeft,. Ook in deze situatie is het nodig om een FG aan te stellen. Meestal is een po betrokken bij de voorbereiding en uitvoering van bijvoorbeeld projecten en implementatie van wetgeving. Dat is lastig te verenigen met de functie van FG. Ook kan het voorkomen dat de po eindverantwoordelijk is voor het organiseren en garanderen van privacy binnen een organisatie. De po is nauw betrokken bij de uitvoering. Dat kan een FG niet: die kan vanwege diens toezichthoudende rol niet diepgaand de eigen werkzaamheden controleren. De werkzaamheden van een po worden juist wel gecontroleerd door de FG. De po en FG werken doorgaans nauw samen.

Een praktijkvoorbeeld van het inzetten van privacy officers, is een organisatie die op iedere vestiging (onderwijslocatie) een po aanstelt waar collega’s met vragen terecht kunnen. Voor alle x vestigingen samen, is er 1 FG die nauw met de po’s samenwerkt. Zo kan de FG voor vragen terecht bij een po op iedere vestiging.

De taken en verantwoordelijkheden voor deze po, komen niet overeen met die van een FG. Voor een po gelden geen wettelijke eisen en voorwaarden, de po heeft geen wettelijke status, en een po heeft ook geen ontslagbescherming. Het komt wel voor dat organisaties, in afwachting van of ter voorbereiding op de komst van een FG, (tijdelijk) een po aanstellen. Ook wordt er wel eens gebruik gemaakt van de rol van privacy officer als een medewerker geen FG kan of mag worden (denk bijvoorbeeld aan het hoofd administratie die wel veel kennis heeft over privacy, maar in verband met het hebben van een dubbel pet, geen FG kan worden).

In het mbo wordt de rol van privacy officer vaak ingevuld door de IBP-manager of – minder voorkomend - adviseur IBP. Meer informatie over diens taken is te vinden in het Framework ibp voor het mbo 2.0.

Vooral voor grotere Colleges van Bestuur is het interessant naast een FG, een IBP-manager of po aan te stellen. Deze medewerker houdt zich dan bezig met de uitvoering van alles wat privacy aangaat, terwijl de FG controleert of het bestuur (en de po of IBP-manager) de privacywet- en regelgeving naleeft. Omdat ‘een slager zijn eigen vlees niet mag keuren’, kan het aanstellen van een po (naast de FG) soms dus wenselijk zijn.

* 1. **Interne of externe FG**

Het is niet noodzakelijk dat een FG in loondienst is bij het College van Bestuur. De AVG kent nadrukkelijk de mogelijkheid om ook een externe FG te benoemen. Er zijn bedrijven die diensten zoals ‘FG-as-a-service’ aanbieden. De FG wordt voor een aantal uur ingehuurd en is bij calamiteiten oproepbaar. De eis is wel dat deze FG “vanuit elke vestiging makkelijk te contacteren is”: de FG moet benaderbaar zijn voor medewerkers en klanten (betrokkenen). Een FG is niet alleen voor externen een aanspreekpunt, maar adviseert en informeert ook de interne organisatie. Maar omdat een externe FG op afstand minder betrokken is bij een organisatie, is het verstandig om regelmatig contact te hebben en de FG langs te laten komen. Een FG die in naam aangewezen is voor de onderwijsinstelling en éénmaal per jaar langs komt voor een gesprek met het College van Bestuur (ook wel ‘postbus-FG’ genoemd), is dus geen optie. De toezichthouder eist dat een FG betrokken is bij de organisatie waar hij werkzaam voor is. Dat kan niet als een FG enkele dagen *per jaar* langs komt of contact heeft. Het verdient aanbeveling dat de FG minstens éénmaal per kwartaal contact heeft met het College van Bestuur.

Voor een kleinere mbo-instelling geldt in de praktijk dat een FG minimaal 0.1 FTE per week werkzaam moet zijn voor de school, ongeacht of dit een externe of een interne FG betreft. Naarmate de grootte van de organisatie toeneemt, zal de omvang van de inzet ook stijgen tot maximaal 1.0 FTE. Daarnaast is de omvang van de inzet afhankelijk van de eisen en wensen van de opdrachtgever. In organisaties waar er bijvoorbeeld geen aparte privacy officer of IBP-manager is, zal een grotere inzet van de FG nodig zijn.

Bij het inschakelen van een externe FG, moeten er goede afspraken worden gemaakt over diens taken en bevoegdheden. Het reglement voor de FG kan daarbij helpen. Ook mag het niet te gemakkelijk zijn voor een College van Bestuur om een extern ingehuurde FG te ontslaan bij een onwelgevallig advies. In die lijn kan een FG gezien worden als een accountant die ook kritisch kijkt naar de jaarrekening en daar een oordeel over geeft, zonder dat de accountant hoeft te vrezen voor zijn opdracht als hij kritische kanttekening plaats.

De AVG noemt de mogelijkheid dat een FG wordt aangewezen die werkzaam is bij een verwerker (leverancier), maar dan moeten de taken en verantwoordelijkheden wel goed geregeld zijn, en is een goede overeenkomst daarvoor noodzakelijk. En er mag natuurlijk geen belangenconflict (kunnen) zijn. Voor het onderwijs wordt deze mogelijkheid vanwege de verschillende (tegenstrijdige) belangen, afgeraden, omdat onafhankelijkheid niet goed te borgen is.

* 1. **Samenwerking tussen besturen**

De AVG biedt ook de mogelijkheid dat verwerkingsverantwoordelijken (Colleges van Bestuur) samenwerken en samen één of meerdere FG’s aanwijzen. Belangrijk is dat een FG vanuit elk bestuur en vestiging makkelijk te bereiken is. Dit moet wel passen bij het type organisatie en praktisch uitvoerbaar zijn, zo lijkt het op het eerste gezicht minder voor de hand te liggen voor een onderwijsinstelling in Noord-Holland om een FG aan te wijzen die gevestigd is in Limburg.

Voor de juridische duidelijkheid en goede organisatie wordt aangeraden de taken binnen de samenwerkende besturen duidelijk te verdelen en voor elk bestuur één persoon als hoofdcontactpersoon (als coördinator) aan te wijzen. Denk hierbij aan de mogelijkheid om per College van Bestuur iemand aan te wijzen met privacy in het aandachtsgebied (bijvoorbeeld als privacy officer, zie paragraaf 3.6).

Het samen met meerdere (kleinere) onderwijsinstellingen regelen van een FG, wordt door de sectorraden gezien als praktische oplossing. Ook als er wordt samengewerkt tussen vo- en mbo-instellingen biedt dit kansen voor het inschakelen van een gezamenlijke FG.

Zeker na invoering van de AVG zal het soms zoeken zijn naar de juiste rolverdeling en taakbelasting van een FG. De sectorraden, saMBO-ICT en Kennisnet brengen deze oplossing dan ook graag onder de aandacht als alternatief voor de vooral kleinere besturen die ook een FG moeten regelen en daar zelf niet de mogelijkheid of middelen voor hebben.

* 1. **Bekend maken aanwijzen FG**

Op basis van de AVG is het vereist dat het bestuur de contactgegevens van de FG publiceert en de contactgegevens aan de relevante toezichthouders communiceert (zie paragraaf 3.5.1). Het doel van deze vereisten is erop toe te zien iedereen binnen en buiten het College van Bestuur, én de toezichthouder gemakkelijk, direct en vertrouwelijk contact met de FG op kan nemen. Het is verplicht deze gegevens op te nemen op de website van het bestuur, en ook op de sites van alle individuele mbo-instellingen die onder het bestuur vallen.

De contactgegevens van de FG dienen informatie te bevatten die betrokkenen en de toezichthouders in staat stellen de FG gemakkelijk te bereiken (postadres, een speciaal telefoonnummer en een speciaal e-mailadres). Waar dit voor de communicatie met het publiek passend is, kunnen ook andere communicatiemiddelen geboden worden, zoals een speciale hotline of een speciaal aan de FG geadresseerd contactformulier op de website van de organisatie.

Een bijzonderheid bij de bekendmaking van de FG, is dat de *naam* van de FG niet hoeft te worden vermeld (maar dat is soms wel zo praktisch).

* 1. **Aansprakelijkheid**

Een FG houdt toezicht op de verwerking van persoonsgegevens en naleving van de AVG. De FG is niet persoonlijk aansprakelijk als er binnen een organisatie een overtreding van de privacywet is[[3]](#footnote-4).

Het feit dat de FG er op toeziet dat de AVG wordt nageleefd, wil niet zeggen dat hij persoonlijk verantwoordelijk is wanneer hier niet aan voldaan wordt. Als *werknemer* blijft de werkgever verantwoordelijk en aansprakelijk voor het werk dat een werknemer uitvoert. De AVG maakt in artikel 24 lid 1 duidelijk dat het niet de FG, maar de verantwoordelijke is die verplicht is “passende technische en organisatorische maatregelen te treffen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd”. Naleving van regels op het gebied van gegevensbescherming is een bedrijfsverantwoordelijkheid van de verwerkingsverantwoordelijke (bestuur) en niet van de FG.

In het geval dat er gebruik wordt gemaakt van een FG die niet als werknemer aan het College van Bestuur verbonden is, is het verstandig om aanvullend afspraken te maken over aansprakelijkheid en om zo nodig/gewenst een verzekering af te sluiten. Of de FG iets mogelijk over het hoofd heeft gezien bij zijn controle of niet, leidend is dat het College van Bestuur verantwoordelijk (en aansprakelijk) is voor naleving van de AVG. Het College van Bestuur zal een boete van de AP niet kunnen doorschuiven naar de extern ingehuurde FG.

1. **Taken en bevoegdheden FG**

*Dit hoofdstuk beschrijft wat de taken en bevoegdheden van de aangewezen FG zijn*

* 1. **Taken FG**

Volgens artikel 39 van de AVG, vervult de FG ten minste de volgende taken:

1. Het bestuur, directie(s) en de werknemers die persoonsgegevens gebruiken, informeren en adviseren over hun verplichtingen ten aanzien de wettelijke vereiste bescherming van persoonsgegevens.
2. Toezien op naleving van:
	1. de AVG,
	2. de andere Unierechtelijke (lees: Europese) of nationale gegevensbeschermingsbepalingen, en
	3. het beleid van het bestuur met betrekking tot de bescherming van persoonsgegevens (inclusief de verantwoordelijkheden, bewustmaking en opleiding van de medewerkers) en de betreffende audits.

De AVG spreekt er over dat de FG het bestuur ‘bijstaat bij het toezicht op de interne naleving van de AVG’. Om dit goed uit te voeren, kunnen FG’s onder andere:

1. informatie verzamelen om het (type) gebruik van persoonsgegevens te identificeren;
2. analyseren en controleren in hoeverre het gebruik van persoonsgegevens aan de AVG voldoet; en
3. het bestuur informeren, adviseren of aanbevelingen geven.
4. Gevraagd en ongevraagd advies geven met betrekking tot de gegevensbeschermingseffect-beoordeling (data protection impact assessments; DPIA) en toezien op de uitvoering daarvan in overeenstemming met de AVG (zie het Framework ibp voor het mbo voor een toelichting hierop).
5. Met de Autoriteit Persoonsgegevens (AP) samenwerken en voor de AP optreden als contactpunt inzake met verwerking van persoonsgegevens verband houdende aangelegenheden, en – waar passend - overleg plegen over enige andere aangelegenheid aangaande privacy.
6. De FG is verplicht bij de uitvoering van zijn taken rekening te houden met de aan het gebruik van persoonsgegevens verbonden risico’s, en met de aard, de omvang, de context en de doelen van het gebruik van die gegevens.
	1. **Uitvoering taken**

Volgens artikel 38 AVG is het een eis dat het bestuur de FG “naar behoren en tijdig betrekt bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens”. De FG moet autonoom binnen de organisatie kunnen functioneren. Vooral bij risico-inventarisaties of gegevensbeschermingsbeoordelingen (DPIA) is het belangrijk dat de FG daar in een vroeg stadium bij betrokken is.

Daarnaast is het belangrijk dat de FG als een gesprekspartner binnen de organisatie gezien wordt en dat hij of zij deel uitmaakt van de relevante werkgroepen die binnen de instelling gegevens verwerken.

Praktische tips om er voor te zorgen dat de FG goed op de hoogte is van wat er speelt, zijn:

* Nodig de FG regelmatig uit voor directie- en bestuursvergaderingen, en desgewenst locatie- en teamvergaderingen.
* Zorg dat de FG aanwezig is als er beslissingen worden genomen die gevolgen kunnen hebben voor de privacy van studenten en medewerkers. Beter is het om de FG in een vroeg stadium te betrekken bij de besluitvorming zodat eventuele adviezen gelijk meegenomen kunnen worden (denk bijvoorbeeld bij inkoop- of aanbestedingsoverwegingen).
* Leg schriftelijk vast wat de adviezen van de FG zijn, en als die niet gevolgd (kunnen) worden.
* De FG moet direct betrokken worden bij een beveiligingsincident of (mogelijk) datalek.
* Zorg dat in procedures is vastgelegd of en wanneer de FG geïnformeerd wordt (bespreek of en wanneer bijvoorbeeld notulen of agenda worden gedeeld).
	1. **Bevoegdheden**

De AVG verplicht het bestuur om de FG toegang te geven tot alle persoonsgegevens en verwerkingen daarvan. Ook moet de FG de benodigde middelen ter beschikking hebben om zijn taken uit te kunnen voeren en om zijn deskundigheid in stand te houden. De FG moet bij zijn werk actief ondersteund worden door ‘het hoger management’.

Om het werk van de FG zo praktisch mogelijk te maken, worden de volgende uitgangspunten aangehouden:

* Voldoende tijd voor de FG om zijn taken te vervullen;
* Voldoende steun qua financiële middelen, infrastructuur (terrein, faciliteiten, apparatuur);
* Officiële communicatie binnen de organisatie over de aanwijzing van de FG zodat het bestaan en functie van de FG bekend is;
* Vereiste toegang tot andere diensten, zoals toegang tot de bestanden van personeelszaken, de eventueel aanwezige jurist, de ICT-afdeling (of met ict-belaste medewerker), etc. De FG ontvangt van deze medewerkers of afdelingen de essentiële steun, input en informatie;
* De FG moet de mogelijkheid hebben om bij te blijven op het gebied van gegevensbescherming, waarbij het uitgangspunt moet zijn dat het kennisniveau continue toeneemt;
* De FG is bevoegd om – op eigen initiatief – onderzoek uit te voeren, daarover (ongevraagd) te adviseren, en om van iedereen in de organisatie medewerking daaraan te eisen.
1. **Expertise, functie-eisen en rechtspositie FG**

*Dit hoofdstuk beschrijft het profiel van een FG en aan welke eisen de FG moet voldoen.*

* 1. **FG als professional**

De FG wordt volgens artikel 37 lid 5 AVG aangewezen op grond van zijn:

* professionele kwaliteiten en
* deskundigheid op het gebied van de wetgeving en
* praktijkkennis inzake gegevensbescherming en
* Kwaliteiten om zijn taken als FG te kunnen vervullen (persoonlijke kwaliteiten zijn bijvoorbeeld integriteit en professionele ethiek).

Dit betekent niet dat een FG persé een juridische opleiding, achtergrond of ervaring moet hebben (al heeft dat wel de voorkeur vanwege het werken met privacywetgeving). De ervaring leert dat een it-beheerder, ict-coördinator, CIO of informatiemanager ook ruime ervaring heeft met ict en het verwerken van persoonsgegevens. Er zijn verschillende opleidingsmogelijkheden voor FG’s om zich verder te bekwamen als deskundige.

De deskundigheid die nodig is wordt namelijk mede bepaald op grond van het gebruik van persoonsgegevens binnen de organisatie (College van Bestuur). Het vereiste kennisniveau moet passen bij de gevoeligheid, complexiteit en de hoeveelheid gegevens die binnen de mbo-instelling worden verwerkt. Als voorbeeld zal een FG binnen een onderwijsinstelling voor speciaal onderwijs (passend onderwijs) meer kennis en expertise over gezondheidsgegevens moeten hebben dan een FG bij een online webwinkel. Over het algemeen geldt dat hoe complexer, omvangrijker en/of gevoeliger de verwerkingen zijn, des te deskundiger (expertise/ervaring) de FG moet zijn.

* 1. **Vereiste expertise en vaardigheden**

De FG moet in ieder geval:

* kennis hebben van nationale en Europese privacywet- en regelgeving;
* begrip hebben van het gebruik van persoonsgegevens binnen de organisatie;
* kennis hebben van ict en informatiebeveiliging;
* de organisatie en onderwijssector kennen (weten hoe er in de onderwijssector met persoonsgegevens wordt omgegaan);
* vaardigheden hebben om binnen de organisatie een cultuur van gegevensbescherming te ontwikkelen.
	1. **Onafhankelijkheid**

De FG is niet alleen adviseur maar ook (intern) controleur. Om zijn werk goed uit te kunnen oefenen, moet een FG onafhankelijk zijn. Deze onafhankelijk is geborgd in de wet, door bijvoorbeeld de wettelijke ontslagbescherming van een FG. De FG mag geen leidende instructies ontvangen van het bestuur die belemmeren dat de FG zijn taken en verplichtingen onafhankelijk kan vervullen. Het bestuur mag een FG geen directe instructies geven over het innemen van bepaalde standpunten bij besluiten, voorstellen of over een bepaald gebruik van persoonsgegevens. De FG moet onafhankelijk zijn en in vrijheid kunnen adviseren.

Overigens blijkt in de praktijk dat de onafhankelijkheid en invulling van de functie van de FG, erg persoonsgebonden is. Zo zal de ene FG zich vrijer voelen om aan te schuiven bij een projectoverleg met softwareontwikkelaars om hen te adviseren, terwijl een andere FG meer afstand wenst te houden om achteraf het projectteam te kunnen controleren. Belangrijk is dat de FG niet alleen formeel onafhankelijk is, maar zich dus ook vrij voelt om onafhankelijk te opereren en adviseren.

* 1. **Ontslagbescherming**

Om er voor te zorgen dat de FG onafhankelijk kan opereren, geniet de FG volgens artikel 38 lid 2 AVG ontslagbescherming. Het bestuur kan en mag een FG niet ontslaan omdat deze kritische adviezen geeft, of het niet eens is met het bestuur. Ook mogen er geen disciplinaire straffen worden opgelegd verband houdende met het werk van de FG en het uitvoeren van diens taken. Hierin is de rechtspositie van een FG vergelijkbaar met die van een lid van de ondernemingsraad.

Uiteraard is het wel toegestaan een FG te ontslaan indien deze niet functioneert, contractuele of arbeidsrechtelijke instructies overtreedt (te denken valt aan psychologische of seksuele intimidatie, misdragingen, diefstal of soortgelijke zware misdragingen). Om misverstanden rondom ontslagbescherming te voorkomen, verdient het aanbeveling om dit proces goed vast te leggen.

**Bijlage 1: Juridische onderbouwing aanwijzen FG**

*Dit hoofdstuk, genummerd als bijlage, geeft de juridische onderbouwing waarom een College van Bestuur (mbo) of schoolbestuur (po/vo) een FG moet aanwijzen.*

1. 1. **Artikel 37 AVG**

De vraag of een College van Bestuur (bevoegd gezag) een FG moet aanwijzen, wordt bepaald door de criteria opgenomen in artikel 37 van de AVG. In het eerste lid van dat artikel staat:

*1.De verwerkingsverantwoordelijke en de verwerker wijzen een functionaris voor gegevensbescherming aan in elk geval waarin:*

*a) de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan, behalve in het geval van gerechten bij de uitoefening van hun rechterlijke taken;*

*b) een verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen; of*

*c) de verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens uit hoofde van artikel 9 en van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10.*

De bepalingen van de AVG worden voorafgegaan door ‘overwegingen’ en een toelichting. Over de FG wordt in punt 97 een toelichting gegeven waarom een FG in deze gevallen noodzakelijk is:

*Indien de verwerking door een overheidsinstantie wordt uitgevoerd, met uitzondering van gerechten of onafhankelijke rechterlijke autoriteiten die handelen in het kader van hun gerechtelijke taken, of indien in de particuliere sector de verwerking door een verwerkingsverantwoordelijke wordt uitgevoerd die als kerntaak heeft verwerkingsactiviteiten uit te voeren die grootschalige regelmatige en systematische observatie van betrokkenen vereisen, indien de verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van persoonsgegevens en van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten, dient een persoon met deskundige kennis van gegevensbeschermingswetgeving en -praktijken de verwerkingsverantwoordelijke of de verwerker bij te staan bij het toezicht op de interne naleving van deze verordening. In de particuliere sector hebben de kerntaken van een verwerkingsverantwoordelijke betrekking op diens hoofdactiviteiten en niet op de verwerking van persoonsgegevens als nevenactiviteit. Het vereiste niveau van deskundigheid dient met name te worden bepaald op grond van de uitgevoerde gegevensverwerkingsactiviteiten 4.5.2016 L 119/18 Publicatieblad van de Europese Unie en de bescherming die voor de door de verwerkingsverantwoordelijke of de verwerker verwerkte gegevens vereist is. Dergelijke functionarissen voor gegevensbescherming dienen in staat te zijn hun taken en verplichtingen onafhankelijk te vervullen, ongeacht of zij in dienst zijn van de verwerkingsverantwoordelijke.*

Bij het bepalen of een College van Bestuur een FG moet aanwijzen, zijn er uit de AVG de volgende criteria te destilleren:

1. De organisatie is aan te merken als *overheidsinstantie of overheidsorgaan* en/of
2. *hoofdzakelijk belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen* vereisen en/of
3. de *verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens uit hoofde van artikel 9 en/of van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10.*

In hoofdstuk 3 is ingegaan op de aparte onderdelen a, b en c.

Helaas wordt in de AVG en de toelichtingen daarop niet gesproken over onderwijsinstellingen, laat staan of zij een FG moeten aanwijzen. Dat betekent dat uit de AVG moet worden afgeleid of een FG verplicht is voor onderwijsinstellingen.

In Europa bestaat gelukkig ook de Artikel 29 werkgroep (Workingparty 29; WP29), vanaf 25 mei 2018 is dit het ‘Europees Comité voor gegevensbescherming’ (European Data Protection Board; EDPB) zoals omschreven artikel 68 AVG genoemd. Het Comité bestaat uit vertegenwoordigers van de nationale privacytoezichthouders en zorgt ervoor dat de AVG consequent wordt toegepast en uitgelegd. Dat doen zij onder andere door het uitvaardigen van richtsnoeren. Deze richtsnoeren geven vaak verduidelijkingen en uitleg over hoe de AVG moet worden toegepast. Op 5 april 2017 zijn de “Richtlijnen voor functionarissen voor de gegevensbescherming (FG’s)” (Guidelines on Data Protection Officers (‘DPOs’))[[4]](#footnote-5) vastgesteld. Die richtlijn geeft meer informatie over de rol en (verplichte) aanstelling van een FG. De richtlijn wordt hierna “Richtlijn FG’s” genoemd.

Volledigheidshalve moet worden vermeld dat, zelfs als een FG niet verplicht zou zijn, altijd *vrijwillig* besloten kan worden tot het aanwijzen van een FG. In dat geval is er geen verschil tussen diens rechten en verplichtingen ten opzichte van een verplicht aangestelde FG.

* 1. **De mbo-instelling als overheidsinstantie of overheidsorgaan**

In de AVG is geen definitie opgenomen over wat wordt verstaan onder het begrip overheidsinstantie of overheidsorgaan. Of sprake is van een dergelijke instantie moet daarom op grond van Europese en Nederlandse wet- en regelgeving worden bepaald. Het kan dus ook gaan om private organisaties die publieke taken uitvoeren.

Bepalend is of een mbo-instelling een publieke taak vervult of met publiek gezag is omkleed. In het Nederlands recht kan daarvoor worden gekeken naar het begrip ‘bestuursorgaan’ uit de Algemene wet bestuursrecht (Awb).

In Nederland worden onderwijsinstellingen niet gezien als overheidsinstanties zoals bedoeld in de Awb. Wel worden mbo-instellingen gezien als semi-overheid: een organisatie die 'dicht tegen de overheid aan zit’ en wettelijke taken en/of het algemeen publiek belang dienen, en publiek gefinancierd zijn. Een aantal delen van het bestuursrecht gelden ook voor openbare mbo-instellingen (die vallen onder het College van B&W). Het geven van onderwijs wordt gezien als zuivere taak van algemeen belang: overbrengen van kennis, vaardigheden en attitudes met vooraf vastgelegde doelen. Hiernaast heeft de overheid overwegende invloed op de inrichting van het onderwijs in Nederland. Zo kennen we de Inspectie van het Onderwijs, en mogen mbo-instellingen zich niet zomaar laten sponsoren of extern laten financieren.

Onderwijsinstellingen worden in veel gevallen wel gelijk gesteld aan publiekrechtelijke instellingen. Zo zijn ze volgens de Aanbestedingswet aanbestedingsplichtig: een verplichting die alleen geldt voor publiekrechtelijke instellingen die specifiek ten doel hebben om te voorzien in behoeften van algemeen belang (anders dan van industriële of commerciële aard), die rechtspersoonlijkheid bezit en waarvan:

* de activiteiten door de staat, provincie, gemeente, waterschap of een andere publiekrechtelijke instelling worden gefinancierd,
* het beheer is onderworpen aan toezicht door de staat, een provincie, een gemeente, een waterschap of een andere publiekrechtelijke instelling of
* de leden van het bestuur, het leidinggevend of toezichthoudend orgaan voor meer dan de helft door de staat, een provincie, een gemeente, een waterschap of een andere publiekrechtelijke instelling zijn aangewezen.

Onderwijsinstellingen voldoen aan ten minste 2 van 3 criteria, waarmee ze vallen onder de aanbestedingsverplichting en daarmee volgens de aanbestedingsregels een publiekrechtelijke instelling zijn.

In de AVG (overweging 154) en de Richtlijn FG’s wordt gerefereerd aan Richtlijn 2003/98/EG die gaat over toegang van het publiek tot officiële documenten. Deze richtlijn geeft een duidelijker definitie van publiekrechtelijke instelling. Het gaat dan om iedere instelling die:

* is opgericht met het specifieke doel om te voorzien in behoeften van algemeen belang die niet van industriële of commerciële aard zijn, en
* rechtspersoonlijkheid heeft, en
* waarvan
	+ óf de activiteiten in hoofdzaak door de staat of zijn territoriale lichamen of andere publiekrechtelijke instellingen worden gefinancierd,
	+ óf het beheer is onderworpen aan toezicht door deze laatste, hetzij de leden van het bestuursorgaan, het leidinggevend orgaan
	+ óf het toezichthoudend orgaan voor meer dan de helft door de staat, zijn territoriale lichamen of andere publiekrechtelijke instellingen zijn aangewezen.

Ook op basis van deze criteria is de conclusie gerechtvaardigd dat onderwijsinstellingen onder de definitie van publiekrechtelijke instelling kunnen vallen: overheidsinstantie of –orgaan.

In de Richtlijn FG’s wordt verder een vergelijking gemaakt met organisaties die overheidstaken uitvoeren zoals bijvoorbeeld het openbaar vervoer, water- en energievoorziening, infrastructuur, de publieke omroep, huisvesting of disciplinaire instanties voor beschermde beroepen. Ondanks dat deze organisaties geen publieke instellingen zijn, kunnen private rechtspersonen wel publieke taken uitvoeren. Deze organisaties kunnen daarmee gezien worden als ‘overheidsinstantie’. Betrokkenen bevinden zich wellicht in vrijwel dezelfde situatie als diegenen van wie gegevens door een ‘zuivere’ overheidsinstantie of -orgaan verwerkt worden: ze hebben geen keuze om gegevens niet te delen. De betrokkenen hebben doorgaan geen keus om hun gegevens te laten verwerken, en er is meestal wetgeving die verplicht om gegevens te verwerken (in centrale databases). De Richtlijn FG’s noemt het een ‘good practice’ om deze privaatrechtelijke organisaties die overheidstaken verrichten te verplichten een FG aan te laten wijzen.

Onderwijsinstellingen kwalificeren niet als overheidsinstanties of overheidsorganen. Alhoewel zij vanwege hun publiekrechtelijke en wettelijk taak daar wel aan gelijk gesteld worden, ligt dat niet voor de hand. Dit neemt niet weg dat in Europees verband wordt aanbevolen dat organisatie, die niet letterlijk kwalificeren als een overheidsinstantie of –orgaan, toch een FG kunnen aanwijzen.

Gezien de vrijheid van onderwijs zoals die in de Grondwet is geborgd, ligt het niet voor de hand om een FG aan te stellen op basis van artikel 37 lid 1 sub a AVG. In omliggende Europese landen is onderwijs doorgaans wel geregeld door of vanwege de overheid, zodat voor die landen een aanwijzing van een FG op deze grond meer voor de hand ligt dan voor de Nederlandse situatie.

* 1. **Hoofdzakelijk belast met regelmatige en stelselmatige observatie op grote schaal**

Artikel 37 lid 1 sub b AVG geeft een aantal criteria op basis waarvan een organisatie een FG moet aanwijzen: de organisatie is *hoofdzakelijk belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen*. Hieronder wordt per begrip beoordeeld of onderwijsinstellingen onder deze bepaling vallen.

* + 1. **Hoofdzakelijk belast: kerntaken**

Bij dit criterium gaat het om de hoofdactiviteiten van de organisatie, en niet op de verwerking van persoonsgegevens als nevenactiviteit. “*Hoofdzakelijk belast met*” of “*kerntaken*” zijn volgens de Richtlijn FG’s de belangrijkste handelingen die nodig zijn om het doel/taak van die organisatie te bereiken. Hier vallen ook activiteiten onder waarbij de verwerking van gegevens een onlosmakelijk onderdeel zijn van de werkzaamheden van een organisatie. Als voorbeeld wordt het ziekenhuis genoemd met de kerntaak het bieden van gezondheidszorg, terwijl een ziekenhuis niet in staat is veilige en effectieve gezondheidszorg te bieden zonder medische gegevens vast te leggen. In dit voorbeeld is het verwerken van deze medische gegevens een van de kerntaken van een ziekenhuis, en moet het ziekenhuis een FG aanwijzen.

De vergelijking met een ziekenhuis is voor het onderwijs treffend. Terwijl de kerntaak van een onderwijsinstelling lesgeven en het leren en begeleiden van studenten is, is het daarvoor noodzakelijk om gegevens over dat leerproces vast te leggen. De voortgang wordt voortdurend vastgelegd, en regelmatig wordt daarover gerapporteerd aan student en ouders (rapporten). Sterker nog: verschillende onderwijswetten verplichten tot het vastleggen en uitwisselen van verschillende categorieën persoonsgegevens. Zo is ook de onderwijsovereenkomst een verplicht onderdeel. Andersom geredeneerd is het *onmogelijk* om met de huidige wet- en regelgeving onderwijs te geven *zonder* gegevens vast te leggen.

* + 1. **Op grote schaal**

De AVG kent geen criteria of exacte cijfers om te bepalen wat een verwerking van persoonsgegevens op grote schaal is. Volgens de Richtlijn FG’s kan hierbij wel rekening worden gehouden met de volgende criteria:

1. het aantal betrokkenen – in specifieke cijfers of als percentage van de betreffende bevolking;
2. de hoeveelheid gegevens en/of de hoeveelheid verschillende gegevens die wordt verwerkt;
3. de duur of permanentie van de gegevensverwerking;
4. de geografische reikwijdte van de verwerking.

Het wordt met deze criteria niet op voorhand duidelijk of er sprake is van een grootschalige verwerking van een kleine mbo-instelling. Daartegenover leggen álle basismbo-instellingen in Nederland wel van álle studenten nagenoeg de zelfde informatie vast (mede ingegeven door onderwijswetten die de categorieën te verzamelen persoonsgegevens verplicht stelt). Met ruim 2,4 miljoen studenten in het po, vo en mbo, kan beredeneerd worden dat het onderwijs gaat om een substantieel deel van de bevolking (14,6%) wiens persoonsgegevens worden verwerkt. Een omvang die rechtvaardigt dat extra toezicht op de verwerking van persoonsgegevens geïndiceerd is.

Grootschalig beoordelen in een kwantitatief perspectief, is lastig. Terwijl de grotere mbo-instellingen (met meerdere locaties) persoonsgegevens verwerken van tienduizenden studenten, zijn die persoonsgegevens inhoudelijk niet anders of minder gevoelig dan bij de kleinste mbo-instelling.

Een beter aanknopingspunt zijn de *duur*, *hoeveelheid* en *verscheidenheid* in gegevens die worden verwerkt. Gedurende de gehele mbo-instellingloopbaan worden er persoonsgegevens van studenten verzameld, vastgelegd, geregisterd en bij de overstap van po naar vo zelfs verplicht uitgewisseld (onderwijskundig rapport). Hierbij kan gekeken worden naar het toonaangevend onderzoek van de Autoriteit Persoonsgegevens in de onderwijssector, het onderzoeksrapport naar Snappet[[5]](#footnote-6). De door de leverancier Snappet verzamelde gegevens van leerlingen (in het po) betreffen “gevoelige persoonsgegevens waaraan allerlei conclusies kunnen worden verbonden met gevolgen in het (latere) maatschappelijk leven”. Naarmate de gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden er zwaardere eisen gesteld aan de beveiliging en het gebruik van deze gegevens. Het oordeel van de AP gaat slechts over de gegevens die één leverancier van digitaal leermateriaal heeft verzameld. Mbo-instellingen maken doorgaans gebruik van meerdere systemen waarin persoonsgegevens van studenten en medewerkers zijn opgeslagen, waarbij deze systemen ook gekoppeld zijn met elkaar. Studentgegevens worden in ‘cockpits’, administratiesystemen en studentvolgsystemen samengebracht. Daarnaast beschikken mbo-instellingen in hun administraties onder meer over informatie over sociaal-emotionele ontwikkeling of medische gegevens. Daarmee kan snel worden aangenomen dat mbo-instellingen beschikken over grote verzamelingen van gevoelige en soms bijzondere persoonsgegevens, waaraan allerlei conclusies verbonden kunnen worden die van grote invloed zijn op de privacy van de betrokken studenten en hun verdere toekomstige opleiding(en) en werk.

Voorbeelden van grote schaal die de Richtlijn FG’s noemt, zijn verwerking van patiëntgegevens in een ziekenhuis, verwerking van reisinformatie van reizigers met het openbaar vervoer in een bepaalde stad, verwerking van klantgegevens bij een verzekeringsmaatschappij of bank, verwerking van gegevens (inhoud, verkeer, locatie) door telefoon- of internetproviders. Hier staat tegenover dat verwerking van patiëntgegevens door een zelfstandig gevestigde arts of verwerking van persoonsgegevens over veroordelingen en strafbare feiten door een individuele advocaat *niet* gezien wordt als een grootschalige verwerking (de Autoriteit Persoonsgegevens noemt dit ‘eenpitters’).

Er wordt overigens niet uitgesloten dat er in te toekomst duidelijker objectieve, kwantitatieve criteria ontwikkeld worden om te bepalen of er sprake is van een verwerking van persoonsgegevens op grote schaal. In de Tweede Kamer is gediscussieerd over een motie om kleine organisaties (mkb) en kleine schoolbesturen (‘éénpitters’) in het po vrij te stellen van de plicht een FG aan te wijzen, deze motie heeft geen gevolg gekregen.

* + 1. **Regelmatige en stelselmatige observatie**

Regelmatige en stelselmatige observatie van betrokkenen gaat over het monitoren (en vastleggen) van het gedrag van de betrokkenen. Regelmatig gaat over voortdurend of gedurende een bepaalde periode, met bepaalde tussenpozen, terugkerend of op vaste tijden herhalend, constant of periodiek observeren. Stelselmatig ziet op het gebruik van systematiek, georganiseerd systeem (zoals een studentadministratie- of studentvolgsysteem), als onderdeel van een algemeen plan voor het gebruik van gegevens of als onderdeel van een strategie.

Zoals al in paragraaf 1.3.1 is besproken, is het verwerken van persoonsgegevens onlosmakelijk verbonden met het onderwijsproces op mbo-instellingen. Docenten observeren hoe hun studenten acteren en vorderingen maken in de klas, leggen dat vast in systemen, passen onderwijs aan op basis van hun bevindingen, en bespreken de voortgang (observaties) met de studenten, en (soms) met hun ouders of de stagebegeleiders.

Het observeren en monitoren is vergelijkbaar met profilering op internet: op basis van eerdere zoekopdrachten worden er nieuwe of andere advertenties getoond. Zo wordt ook in het onderwijs op basis van de observaties les of onderwijs aangepast aan de student (ondersteuningsbehoefte). Studenten met gebleken of gemelde leerachterstanden krijgen extra begeleiding en zorg.

Goed onderwijs in Nederland zonder het monitoren en observeren van studenten, is niet mogelijk. Daarmee wordt voldaan aan het criterium van regelmatige en stelselmatige observatie.

* + 1. **Aard, omvang en/of doeleinden van de verwerking van persoonsgegevens**

In het onderwijs worden er veel gegevens van en over studenten (en soms hun ouders) verwerkt. Blijkens het Besluit uitwisseling leer- en begeleidingsgegevens gaat het – tenminste – om de volgende categorieën gegevens:

a. administratieve gegevens;

b. gegevens over onderwijshistorie, leerresultaten en stage- en werkervaring;

c. gegevens over de sociaal-emotionele ontwikkeling en het gedrag;

d. gegevens met betrekking tot de gegeven of geïndiceerde begeleiding;

e. gegevens omtrent de verzuimhistorie.

* 1. **Grootschalige verwerking van bijzondere categorieën persoonsgegevens en/of strafrechtelijke veroordelingen en strafbare feiten**

In artikel 37 lid 1 sub c AVG wordt een derde criterium gegeven op basis waarvan organisaties een FG moeten aanwijzen. Dat is het geval als de *verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met grootschalige verwerking van*

* *bijzondere categorieën van gegevens uit hoofde van artikel 9 en/of*
* *van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10*.

Voor de bespreking van hoofdzakelijk en grootschalige verwerking van persoonsgegevens, wordt verwezen naar paragraaf 1.3.1 respectievelijk 1.3.2.

Bij deze categorie verwerkingen gaat het om het gebruik van bijzondere persoonsgegevens (deze worden beschreven in artikel 9 AVG). Indien onderwijsinstellingen zich dus veel bezig houden met bijzondere persoonsgegevens zoals medische gegevens, moeten zij een FG aanwijzen. Het gaat hier voornamelijk om wat in het po en vo speciaal onderwijs wordt genoemd: leerlingen worden hier alleen geplaatst om redenen van (voornamelijk) sociaal-emotionele of medische aard. Terwijl in het po en vo hier speciaal onderwijs voor is ingericht, geldt in het mbo een zorgplicht voor studenten die extra steun en begeleiding nodig hebben (Wet gelijke behandeling handicap en chronische ziekte). Mbo-instellingen moeten op grond van deze wet voor iedere student met een beperking doeltreffende aanpassingen realiseren, tenzij dit een onevenredige belasting vormt voor de school. Dit betekent dat ook mbo-instellingen voor deze studenten meer dan de regulier gegevens gebruiken.

Ook kent het onderwijs in Nederland penitentiaire (jeugd)inrichtingen waar mbo-onderwijs wordt gegeven. Daarbij zijn opleidingen of onderwijsinstellingen in of verbonden aan justitiële jongereninrichtingen of gesloten jeugdzorginstellingen. In de eerste categorie instellingen worden persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten verwerkt. In gesloten jeugdzorginstellingen speelt er vaak complexe problematiek die sociaal-emotionele of medische persoonsgegevens omvat (eventueel gecombineerd met strafrechtelijke veroordelingen en strafbare feiten).

Aangezien mbo-instellingen zich niet specifiek richten op het verwerken van gezondheidsgegevens, is het niet aannemelijk dat deze grond om een FG aan te wijzen geldt voor mbo-instellingen.

* 1. **Moet volgens de wet een FG aangewezen worden?**

Op basis van een analyse van de wetgeving (die is opgenomen als bijlage 1) is de conclusie dat een College van Bestuur - vanaf 25 mei 2018 – wel een FG dient aan te wijzen op grond van de AVG, artikel 37 lid 1 sub:

1. Het College van Bestuur is aan te merken als of gelijk te stellen aan een *overheidsinstantie of overheidsorgaan;*
2. Het College van Bestuur is hoofdzakelijk *belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen* vereisen.
	1. **Uitzondering: geen FG aanwijzen**

Het College van Bestuur moet zelf beoordelen of zij onder de hiervoor beschreven criteria vallen. Alhoewel het advies is om wel een FG aan te wijzen, kan een College van Bestuur concluderen dat zij niet voldoet aan de criteria die leiden tot de verplichting om een FG aan te wijzen. Dat besluit dient (schriftelijk) gemotiveerd te worden. Daarbij moet er rekening worden gehouden met de mogelijkheid dat de Autoriteit Persoonsgegevens dit standpunt niet deelt en stelt dat het bestuur toch een FG dient aan te wijzen.

Het is mogelijk dat de in de AVG genoemde criteria in de toekomst worden verduidelijk, bijvoorbeeld door een nieuwe Richtlijn FG’s die exacte cijfers als criterium geeft voor de hoeveelheid betrokkenen, medewerkers of gegevens die verwerkt zou moeten worden. Er wordt niet uitgesloten dat er een standaard ontwikkeld kan worden voor het bepalen van objectieve, kwantitatieve criteria voor wat, met betrekking tot bepaalde, veelvoorkomende verwerkingsactiviteiten, als ‘grootschalig’ gezien wordt. Er wordt aan gedacht om voorbeelden van ondergrenzen voor de aanwijzing van een FG te delen en publiceren. Criteria zoals omvang, hebben eerder wel in concept-teksten van de AVG gestaan: een organisatie groter dan 5.000 betrokkenen moest een FG moest aanwijzen, of al de organisatie een omvang had van meer dan 250 medewerkers. Deze criteria zijn – bewust – geschrapt zodat die geen houvast meer bieden, maar niet moet worden uitgesloten dat soortgelijke criteria alsnog gebruikt kunnen worden.

Ook als het College van Bestuur van mening is dat de AVG het aanstellen van een FG niet specifiek verplicht stelt, kan het voor het College van Bestuur zinvol zijn vrijwillig een FG aan te wijzen. In de Richtlijn FG’s moedigt de Artikel 29-werkgroep (EDPB) deze vrijwillige keuze aan.

Belangrijk uitgangspunt bij het innemen van een uitzonderingspositie zijn:

* Het bestuur moet altijd kunnen uitleggen waarom er (tijdelijk) voor gekozen is om geen FG aan te wijzen (comply of explain). Documenteer deze beslissing altijd, dit sluit aan bij het begrip van ‘accountability’ dat uitgangspunt is in de AVG.
* Als de conclusie is dat een bestuur niet zelf een FG wil of kan aanwijzen, moet overwogen worden of een samenwerking met/tussen meerdere (kleine) besturen (on)mogelijk is: de AVG biedt expliciet ruimte dat organisaties samen één FG regelen.

**Bijlage 2: Regeling taken en bevoegdheden FG**

*In dit hoofdstuk is een voorbeeldreglement opgenomen dat de verwerkingsverantwoordelijke dient vast te stellen gelijktijdig met het aanwijzen van een FG. Hierbij is gebruik gemaakt van een voorbeeld dat gebaseerd is op de \*AVG\* en is aangepast aan de terminologie van de AVG.*

De GEEL GEARCEERDE TEKST MOET NOG AANGEPAST WORDEN

**Regeling taken en verantwoordelijkheden Functionaris voor Gegevensbescherming**

**Artikel 1: definities**

a. AVG: Algemene Verordening Gegevensbescherming;

b. FG: functionaris voor gegevensbescherming zoals bedoeld in artikel 37 van de AVG;

c. Verwerkingsverantwoordelijke: het College van Bestuur van [naam mbo-instelling]

d. Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, bedrijf, organisatie, een dienst of een ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke persoonsgegevens verwerkt;

e. Persoonsgegeven: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (betrokkene) waarbij als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

f. Verwerking van persoonsgegevens: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

g. Personeel: medewerkers in loondienst en/of extern ingehuurde medewerkers die in opdracht van de Verwerkingsverantwoordelijke werkzaamheden verrichten.

**Artikel 2: Taken**

1. De FG heeft de volgende taken:
	1. het houden van toezicht op verwerkingen van persoonsgegevens;
	2. toezicht op wijzigingen in bestaande verwerkingen en/of het aanleggen van nieuwe verwerkingen met persoonsgegevens binnen [mbo-instelling];
	3. geven van (ongevraagd) advies en doen van aanbevelingen over privacy in het algemeen en de toepassing van de AVG;
	4. overleg met (de contactpersoon van) de Autoriteit Persoonsgegevens;
	5. het toezicht houden op het verwerkingsregister (dataregister) met alle verwerkingen persoonsgegevens binnen [mbo-instelling];
	6. het (laten) afhandelen van klachten of vragen van betrokkenen inzake privacy;
	7. overige door het bestuur of directie van [mbo-instelling] aan de FG opgedragen werkzaamheden aangaande privacy;
	8. jaarlijks opstellen van een verslag van zijn werkzaamheden.
2. De FG rapporteert aan het College van Bestuur van [mbo-instelling].
3. Het personeel meldt bij de FG alle (nieuwe) verwerkingen van persoonsgegevens alsmede eventuele incidenten met betrekking tot privacy.
4. De FG heeft binnen [mbo-instelling] een onafhankelijke positie. Het College van Bestuur stelt de FG in de gelegenheid diens taken zelfstandig, onafhankelijk, zonder enige belemmering en naar behoren uit te oefenen. De FG ontvangt voor wat betreft de uitoefening van dienst functie geen aanwijzingen van het College van Bestuur.
5. *OPTIONEEL*: De security officer is betrokken bij de dagelijkse operationele gang van zaken met betrekking tot de diensten en voorzieningen van [mbo-instelling]. De security officer overlegt met en informeert de FG terzake van privacy-gerelateerde kwesties en vraagstukken over de voorzieningen van [mbo-instelling].

**Artikel 3: Bevoegdheden**

1. De FG is bevoegd, zo nodig met medeneming van de benodigde apparatuur, elke plaats in de gebouwen op de terreinen die bij [mbo-instelling] in gebruik zijn en waar persoonsgegevens worden verwerkt, te betreden.
2. De FG is bevoegd inlichtingen te vorderen van een ieder die onder gezag of in opdracht van [mbo-instelling] werkzaam is of overeenkomstig voor of namens [mbo-instelling] persoonsgegevens verwerkt.
3. De FG is bevoegd inzage te vorderen van zakelijke gegevens en bescheiden waarin persoonsgegevens zijn verwerkt.
4. De FG is bevoegd van de gegevens en bescheiden kopieën te maken.
5. Indien het maken van kopieën niet ter plekke kan gebeuren, is hij bevoegd de gegevens en bescheiden voor maximaal één werkdag mee te nemen.
6. De FG is bevoegd tot het geven van een opdracht tot
	1. het aanmaken van een registratie van persoonsgegevens in overeenstemming met de AVG;
	2. vernietiging van persoonsgegevens, waarvan de bewaartermijn is overschreden of indien de gegevensverwerking onrechtmatig is.
7. De FG is bevoegd zich te laten vergezellen en bijstaan door personen die daartoe door hem zijn aangewezen.
8. De FG maakt van de bevoegdheden als bedoeld in dit artikelen slechts gebruik voor zover dit redelijkerwijs voor de uitoefening van de taak noodzakelijk is.

**Artikel 4: Weigering**

1. Een ieder, die werkzaam is bij en/of in opdracht werkt van de verantwoordelijke, is verplicht aan de FG medewerking te verlenen, die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden.
2. Indien de medewerking aan de uitoefening van de bevoegdheden van de FG zoals bedoeld in artikel 3, wordt geweigerd, kan het College van Bestuur, op een met redenen omkleed verzoek, toestemming verlenen aan de FG de benodigde handelingen zelfstandig uit te voeren in weerwil van de weigering tot medewerking.
3. Het bestuur en/of directie van [mbo-instelling] wordt zo spoedig mogelijk in kennis gesteld over de uitvoering van het bepaalde in dit artikel.

**Artikel 5: Geheimhouding**

1. De FG is verplicht tot geheimhouding van al hetgeen hem op grond van deze regeling bekend is geworden, tenzij de betrokkene in bekendmaking toestemt of de FG op grond van wet- en regelgeving verplicht is om de betreffende informatie en daarin begrepen persoonsgegevens bekend te maken of te melden.

**Artikel 6: Regeling**

1. Deze regeling wordt vastgesteld en gewijzigd bij besluit van de Verwerkingsverantwoordelijke.
2. Deze regeling treedt in werking op [datum] en zal intern aan het personeel bekend worden gemaakt door publicatie op [locatie plaatsing reglement].

Vastgesteld door het College van Bestuur van [mbo-instelling] op [datum], versie [versienummer].

**Bijlage 3: voorbeeld vacaturetekst FG**

*Dit is een voorbeeld tekst die gebruikt kan worden bij het opstellen van een vacature voor een FG*.

***Voor [mbo-instelling] zijn we op zoek naar een functionaris voor gegevensbescherming (FG) voor XX uur per week.***

**Functiebeschrijving**

**CONTEXT**

De werkzaamheden worden verricht binnen [mbo-instelling en omschrijving]. De FG adviseert en rapport aan de portefeuillehouder informatiebeveiliging en privacy binnen het College van Bestuur.

Het College van Bestuur streeft naar een maximale kwaliteit van haar informatiebeveiliging en bescherming van privacy, en heeft daartoe een informatiebeveiligings- en privacybeleid opgesteld. De FG opereert zelfstandig binnen het (bestuur/onderwijsinstelling), is onafhankelijk en houdt toezicht op de toepassing en naleving van privacywetgeving zoals de Algemene Verordening Gegevensverwerking (AVG) die per 25 mei 2018 van kracht is geworden. De FG is verantwoordelijk voor het toezicht op de uitvoering van het vastgestelde beleid op het terrein van informatiebeveiliging en privacy en doet voorstellen voor mogelijke verbeteringen op dit terrein. De FG levert een bijdrage aan de rapportages met betrekking tot de stand van zaken van de beveiliging van informatie.

**RESULTAATGEBIEDEN**

1. Resultaatgebied bijdrage aan ontwikkeling instelling breed stelsel van informatiebeveiliging

* Signaleert en rapporteert over de stand van zaken m.b.t. de naleving van de AVG in onderdelen van de instelling aan de betreffende directeur en portefeuillehouder informatiebeveiliging en privacy (ibp) binnen het bestuur;
* Maakt afwijkingen van voorgenoemde voorschriften en regelingen bespreekbaar en maakt afspraken met de verantwoordelijke functionaris;
* Adviseert en ondersteunt onderdelen van de onderwijsinstelling bij de verbetering en evaluaties m.b.t. naleving van de AVG (verloop, inhoud en resultaat) en maakt daarbij gebruik van de PDCA- cyclus;
* Anticipeert op ontwikkelingen binnen een tijdshorizon van maximaal 2 tot 3 jaar.

2. Resultaatgebied uitvoering AVG

* Levert een bijdrage aan het bewaken en evalueren van procedures, planningen en instrumenten met betrekking tot de AVG
* Doet onderzoek naar de naleving van de AVG en het bewaken ervan;
* neemt deel aan overlegvormen, projecten en samenwerkingsverbanden op het gebied van de informatiebeveiliging en privacy;
* Fungeert als aanspreekpunt voor misstanden betreffende de AVG binnen de onderwijsinstelling;
* Levert een bijdrage aan interne en externe rapportages en verantwoordingsdocumenten op het terrein van informatiebeveiliging en privacy;
* Houdt toezicht op, rapporteert over en adviseert over de verwerking van persoonsgegevens binnen alle onderdelen van de organisatie.;
* Draagt zorg voor de toepassing van de AVG en controleert een passend niveau van beveiliging van de informatiehuishouding;
* Adviseert over maatregelen gericht op het beperken van (het gebruik van) persoonsgegevens.
* Behandelt vragen en klachten m.b.t. de AVG;
* Geeft voorlichting over het gebruik van persoonsgegevens en bevordert awareness bij medewerkers rondom hun verplichtingen bij het verwerken van persoonsgegevens;
* Treedt op als intermediair tussen de onderwijsinstelling en de Autoriteit Persoonsgegevens;
* Neemt deel aan overleg over de uitvoering van het IBP-beleid.

3. Resultaatgebied control

* Levert een bijdrage aan de kwaliteit van het niveau van informatiebeveiliging binnen de instelling.
* Levert een bijdrage aan en adviseert over (het initiëren van) informatiebeveiligingsassessments, -tests, -reviews en –audits.
* Levert een bijdrage aan interne en externe jaarrapportages en verantwoordingsdocumenten over het niveau van de informatiebeveiliging.
* Informeert de portefeuillehouder IBP m.b.t de naleving van de eisen m.b.t de Algemene Verordening Gegevensbescherming (AVG).

**KADER, BEVOEGDHEDEN EN VERANTWOORDELIJKHEDEN**

Verantwoording schuldig aan: de portefeuillehouder ibp binnen het College van Bestuur over de kwaliteit van de rapportages m.b.t. de naleving van de AVG, de afspraken met de verantwoordelijke functionaris, de bijdrage aan het ontwerpen, bewaken en evalueren van procedures, planningen en instrumenten en het onderzoek naar de naleving van de AVG.

Kader: De AVG en afgeleide wet- en regelgeving, onderwijswetgeving, kwaliteitsstandaarden, richtlijnen en specifiek geformuleerde beleidslijnen ten aanzien van informatiebeveiliging en privacy.

Beslist over/bij:, de rapportages, interne en externe verantwoordingsdocumenten m.b.t. de naleving van de AVG en adviezen over de verwerking van persoonsgegevens binnen alle onderdelen van de organisatie.

**Kennis en vaardigheden**

De functionaris gegevensbescherming beschikt over de volgende kennis en vaardigheden

• Hbo of wo werk- en denkniveau, bij voorkeur een rechten-opleiding of een relevante HBO/WO-opleiding inzake dataprotectie.

• Algemeen theoretische en praktische kennis van (Informatie)beveiliging en privacywetgeving.

• Kennis van en inzicht in de taak- en doelstelling en de werkwijze van de organisatie van de

onderwijsinstelling.

• Inzicht in de bedrijfs- en onderwijsprocessen binnen de onderwijsinstelling.

• Vaardigheid in het toezicht houden op gebruik van ict-systemen waarbinnen persoonsgegevens worden verwerkt.

• Vaardigheid in projectmatig werken.

• Vaardigheid in het uitvoeren van informatiebeveiligingsassessments, -tests, -reviews en –audits

• Vaardigheid in het opstellen van verbetervoorstellen en adviezen.

• Communicatieve vaardigheden.

**Contacten**

De functionaris gegevensbescherming moet investeren in de volgende relaties:

* Met leden van het College van Bestuur en directeuren (proceseigenaren) van de onderwijsinstelling om met uiteenlopende belangen om te gaan, informatie te geven en de uitvoering af te stemmen;
* Met directeuren (proceseigenaren) van de onderwijsinstelling om informatie te geven en de naleving van de AVG af te stemmen;
* Met directies en medewerkers over de toepassing van richtlijnen, procedures, processen en werkwijzen voor het gebruik van bestaande, aangepaste of nieuwe voorzieningen, methoden en/of technieken op het terrein van informatiebeveiliging om hen te informeren, vragen te beantwoorden
* Met de portefeuillehouder IBP over de wijze waarop de werkzaamheden dienen te worden uitgevoerd, de evaluatie van de resultaten daarvan, verbetervoorstellen en om informatie uit te wisselen en tot afstemming te komen.
1. <https://www.sambo-ict.nl/netwerken/informatiebeveiliging/framework-ibp/> [↑](#footnote-ref-2)
2. <https://kn.nu/IBPonderwijs> [↑](#footnote-ref-3)
3. <https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/functionaris-gegevensbescherming-fg#hoe-kan-een-fg-intern-toezicht-houden-op-het-naleven-van-de-privacywet-5824> [↑](#footnote-ref-4)
4. <http://ec.europa.eu/newsroom/document.cfm?doc_id=44100>, de Autoriteit Persoonsgegevens heeft een officieuze vertaling gemaakt van deze richtlijn: <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtlijnen_fg.pdf> [↑](#footnote-ref-5)
5. <https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013_snappet.pdf> [↑](#footnote-ref-6)