PO RAAD VO RAAD Kennisnet

Handreiking functionaris voor gegevensbescherming SwV PaO

Uitleg over de verplichting om een FG aan te wijzen

Laat ict werken **voor het onderwijs**

Inhoud

1. INLEIDING 4

2. MANAGEMENTSAMENVATTING 5

3. WETTELIJK KADER AANSTELLEN FG 6
   - 3.1. Belangrijke begrippen over privacy 6
   - 3.2. Samenwerkingsverbanden 7
   - 3.3. Wie bepaalt of een FG aangewezen moet worden? 7
   - 3.4. Autoriteit Persoonsgegevens 7
   - 3.5. Moet volgens de AVG een FG aangewezen worden? 8
   - 3.6. Wat als er op 25 mei 2018 nog geen FG is aangewezen? 8
   - 3.7. Uitzonderingen op wettelijke verplichting 8

4. HOE REGEL JE EEN FG? 9
   - 4.1. Aanwijzen FG 9
   - 4.2. Functie 9
   - 4.3. Onafhankelijk 9
   - 4.4. Bekend maken aanwijzen FG 9
   - 4.5. Autoriteit Persoonsgegevens 10
   - 4.5.1. Aanmelding FG 10
   - 4.6. Externe FG 10
   - 4.7. Samenwerking tussen samenwerkingsverbanden 10
   - 4.8. MR 11
   - 4.9. Aansprakelijkheid 11

5. TAKEN EN BEVOEGDHEDEN FG 12
   - 5.1. Taken FG 12
   - 5.2. Uitvoering taken 12
   - 5.2.1. Onafhankelijkheid 13
   - 5.3. Bevoegdheden 13

6. EXPERTISE, FUNCTIE-EISEN EN RECHTSPOSITIE FG 14
   - 6.1. FG als professional 14
   - 6.2. Vereiste expertise en vaardigheden 14
   - 6.3. Ontslagbescherming 14

7. BEST PRACTICES 15
   - 7.1. Zelf een FG aanwijzen 15
   - 7.2. Gezamenlijk een FG aanwijzen 15
   - 7.3. Tijdbesteding 15

BIJLAGE 1: JURIDISCHE ONDERBOUWING AANWIJZEN FG 16
   - 1.1. Artikel 37 AVG 16
   - 1.2. Het samenwerkingsverband als overheidsinstantie of overheidsorgaan 17
   - 1.3. Hoofdzakelijk belast met regelmatige en stelselmatige observatie op grote schaal 18
   - 1.3.1. Hoofdzakelijk belast: kerntaken 18
   - 1.3.2. Aard, omvang en/of doeleinden van de verwerking van persoonsgegevens 19
   - 1.3.3. Op grote schaal 19
   - 1.3.4. Regelmatige en stelselmatige observatie 20
   - 1.4. Grootschalige verwerking van bijzondere categorieën persoonsgegevens en/of strafrechtelijke veroordelingen en strafbare feiten 20
   - 1.5. Moet volgens de wet een FG aangewezen worden? 20

1.6. Uitzondering: geen FG aanwijzen 21

BIJLAGE 2: REGELING TAKEN EN BEVOEGDHEDEN FG 22

BIJLAGE 3: VOORBEELD VACATURETEKST FG 24

BIJLAGE 4: 26

INFORMATIEBEVEILIGINGS- EN PRIVACYBELEID (IBP) 26

VOOR HET SAMENWERKINGSVERBAND 26

VOORWOORD 27

1. HET BELANG VAN INFORMATIEBEVEILIGING EN PRIVACY 28
1.7. De scope van het informatiebeveiligings- en privacybeleid 28
1.8. Het doel van informatiebeveiliging en privacy 28

2. HET BELEID 29
2.1. Voorbeeldrol 29
2.2. Wet- en regelgeving 29
2.3. IBP is overal in verweven 29
2.4. IBP is de verantwoordelijkheid van iedereen 29
2.5. ISO 27001 als basis 29

3. UITVOERING 30
3.1. Bewustzijn 30
3.2. Incidenten en datalekken 30
3.3. Naleving 30
3.4. Actualiteit 30
3.5. Wet- en regelgeving 31
3.6. De vijf vuistregels van privacy 31
3.7. Dataregister 31
3.8. Planning & controle 31

4. ORGANISATIE 32
4.1. Medewerkers 32
4.2. Management 32
4.3. Specifieke verantwoordelijkheden 32

Colofon

Versie 1.0 (26 maart 2018)

Auteurs Harry Nijkamp (Nijkamp Consult), Job Vos, Axel Eissens, Debby Sikking (Kennisnet)

Met dank aan Anne Goris (VO-raad), Maurits Huigsloot (PO-Raad)
Henk Schlingmann, Wim Voorwinden, Paul Valk, Geert van der Sluis, Monique Pleumeekers, Bert Schumacher, Andre Poot, Robert Bos, Janneke Koopmans, Antoon Fens, Sjef Martens, Vincent Bouwers, Robert van Kuijk, Elly Dingemanse, Dirk Linden.

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

1. Inleiding

Vanaf 25 mei 2018 is de *Algemene Verordening Gegevensbescherming (AVG)* van kracht: een Europese wet die direct van toepassing is in alle landen van de Europese Unie.

De AVG is van toepassing in heel Europa en op alle Europese burgers. Bedrijven die zaken doen met Europese burgers, moeten zich ook aan de AVG houden. Ook bedrijven uit Amerika zoals Facebook, Apple, Google of Microsoft die in Europa actief zijn, moeten zich aan de AVG houden. Alle organisaties die persoonsgegevens gebruiken, hebben verantwoordelijkheden en verplichtingen. Ook maakt de AVG-samenwerking tussen alle Europese privacytoezichthouders mogelijk en zijn de maximumboetes die deze toezichthouders kunnen opleggen verhoogd naar 20 miljoen euro, of zelfs 4% van de jaaromzet van een onderneming.

Een ander belangrijk vereiste uit de AVG is dat organisaties intern hun privacy(beleid) moeten organiseren. Privacy heeft een belangrijke plaats binnen organisaties. Een maatregel om dat te bereiken, is volgens de AVG het aanwijzen van een interne privacytoezichthouder. Die persoon wordt *functionaris voor gegevensbescherming (FG)* genoemd. Vanaf 25 mei 2018 is het volgens de AVG in een aantal gevallen verplicht een FG te hebben.

De verplichting om een FG aan te stellen, geldt ook voor de samenwerkingsverbanden Passend Onderwijs (hierna samenwerkingsverbanden). In deze handreiking wordt uitgelegd waarom het aanwijzen van een FG voor het samenwerkingsverband verplicht is, hoe een FG geregeld kan worden, wat diens taken en bevoegdheden zijn en hoe te handelen als er op 25 mei 2018 (nog) geen FG aangewezen is.

Uit de analyse van de tekst van de AVG die in deze handreiking is opgenomen, volgt dat het aanwijzen van een FG op organisatieniveau door samenwerkingsverbanden verplicht is.

Aanpak IBP

Kennisnet heeft samen met de PO-Raad en VO-raad een stappenplan ontwikkeld waarmee scholen informatiebeveiliging en privacy (IBP) op een eenvoudige én gestructureerde wijze kunnen implementeren: de Aanpak IBP. Deze aanpak is hier te vinden: https://kn.nu/IBPonderwijs
Bestuurders van samenwerkingsverbanden kunnen hier inspiratie aan ontlenen. In de bijlage van deze handreiking treft u een aantal voorbeelddocumenten opgesteld voor samenwerkingsverbanden.

Het regelen van een FG is overigens slechts één van de (vele) zaken die het samenwerkingsverband moet doen om te voldoen aan de in de AVG gestelde vereisten.

2. Managementsamenvatting

Het onderwijs maakt steeds beter en meer gebruik van ICT. Daardoor neemt het aantal persoonsgegevens dat scholen en samenwerkingsverbanden gebruiken toe en wordt het beschermen van de privacy van leerlingen en medewerkers steeds belangrijker. Besturen van samenwerkingsverbanden zijn volgens de wet verplicht om privacy goed te regelen.

Op 25 mei 2018 treedt de Europese Algemene Verordening Gegevensbescherming (AVG) in werking die op een aantal punten strenger is dan de Nederlandse Wet Bescherming Persoonsgegevens. Privacy moet volgens deze AVG een belangrijke plaats in de organisatie krijgen en houden. In de Aanpak IBP (https://kn.nu/IBPonderwijs) is een overzicht opgenomen wat scholen nog moeten regelen en waar scholen mee kunnen beginnen om informatiebeveiliging en privacy te regelen. Samenwerkingsverbanden kunnen hier inspiratie uit halen. Daarnaast is een aantal documenten opgesteld voor het samenwerkingsverband. Deze zijn als bijlage bij deze handreiking bijgevoegd.

Een belangrijke wijziging die uit de AVG voortvloeit is dat organisaties in een aantal gevallen verplicht zijn om een functionaris voor gegevensbescherming (FG) aan te wijzen. 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 bestuur van het samenwerkingsverband 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 dan ook voldoende kennis van de organisatie en van privacywetgeving hebben, moet betrouwbaar zijn en moet in onafhankelijkheid zijn werkzaamheden kunnen verrichten. De FG heeft dezelfde ontslagbescherming als leden van de MR.

Uit een juridische analyse van de AVG blijkt dat het samenwerkingsverband verplicht is om een FG “aan te wijzen”. De PO-Raad, VO-raad en Kennisnet adviseren de bestuurders dan ook om een FG aan te wijzen. De aangewezen FG moet worden gemeld bij de toezichthouder voor privacy in Nederland: de Autoriteit Persoonsgegevens.

Het is mogelijk om een medewerker als FG aan te wijzen (intern), of om een FG in te huren (extern). De AVG geeft de mogelijkheid dat organisaties samen een (interne of externe) FG aanwijzen. Voorwaarde daarbij is dat de FG wel de samenwerkende organisaties 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 leerlingen, hun ouders en medewerkers binnen het samenwerkingsverband.

De FG bemoeit zich binnen het samenwerkingsverband met de privacy van medewerkers en leerlingen. Daarom is voorafgaand aan het aanwijzen van een FG, de instemming van de MR van het samenwerkingsverband noodzakelijk. Daarbij gaat het niet om de *persoon* van de FG maar om diens taken, rechten en bevoegdheden.

De verplichting om een FG aan te wijzen is één van de zaken die het bestuur van het samenwerkingsverband moet regelen vanaf 25 mei 2018. Niet alle besturen zullen dan al een FG hebben aangewezen, bijvoorbeeld omdat er nog afspraken moeten worden gemaakt met de samenwerkingsverbanden waarmee samen een FG wordt geregeld of omdat het bestuur eerst de basis onder informatiebeveiliging en privacy wil hebben gelegd. Het advies is dat het bestuur documenteert waarom er (nog) geen FG is aangewezen, en wat de planning is om dat wel te gaan doen. Het is verdedigbaar dat een bestuur van het samenwerkingsverband eerst andere verplichtingen uit de AVG op orde wil hebben gebracht voordat een FG daarop intern toezicht gaat houden.

In deze Handreiking wordt uitgelegd op welke grond een bestuur een FG moet aanwijzen, hoe je die aanwijzing regelt, wat diens taken en bevoegdheden zijn en wat de functie-eisen zijn. Daarnaast worden een aantal praktijkvoorbeelden gegeven over hoe een FG geregeld kan worden.

3. Wettelijk kader aanstellen FG

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

3.1. Belangrijke begrippen over privacy

Om te kunnen voldoen aan de AVG, is het noodzakelijk de basisbegrippen omtrent privacy te kennen.

De AVG gaat over persoonsgegevens. Dat zijn alle gegevens waarmee direct of indirect een natuurlijk persoon (mens) kan worden geïdentificeerd, bijvoorbeeld een naam, BSN, geboortedatum of IP-adres. Ook leerling- en medewerkersgegevens zijn persoonsgegevens. Gevoelige informatie over leerlingen en medewerkers, zoals informatie over gezondheid, gedragsproblemen, politieke voorkeur, godsdienst, seksuele voorkeur of een problematische thuissituatie noemen we bijzondere persoonsgegevens. Met de invoering van de AVG vallen genetische en biometrische gegevens ook onder de categorie bijzondere persoonsgegevens. Bijzondere persoonsgegevens mogen alleen worden verwerkt als daar een wettelijke grond voor is *of* wanneer de betrokkene daar expliciet toestemming voor geeft.

Alles wat er 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: alleen al het gebruiken van persoonsgegevens noemen we verwerken. Kort door de bocht kun je stellen dat het 'aanraken' van persoonsgegevens al verwerken is, zodat de AVG van toepassing is.

De verwerkingsverantwoordelijke is een natuurlijk persoon of instantie die vaststelt welke persoonsgegevens 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. Het Samenwerkingsverband Passend Onderwijs wordt aangemerkt als verwerkingsverantwoordelijke. Net als het bevoegd gezag heeft het samenwerkingsverband een eigen wettelijke taak, stelt zelf de doelen voor de gegevensverwerking en bepaalt zelfstandig met welke middelen de gegevensverwerking uitgevoerd wordt.

De verwerker verwerkt de persoonsgegevens in opdracht van de verwerkingsverantwoordelijke. Een voorbeeld is een samenwerkingsverband dat een digitaal administratiesysteem voor de verwerking van TLV-aanvragen wil gebruiken, en daarvoor een softwarebedrijf inschakelt: als medewerkers inloggen bij het softwarebedrijf, dan verwerkt het bedrijf persoonsgegevens in opdracht van het samenwerkingsverband, het softwarebedrijf is dan verwerker. Omdat de verwerker handelt in opdracht van de verwerkingsverantwoordelijke mag de verwerker alleen verwerkingen doen waarvoor hij uitdrukkelijk opdracht krijgt.

De betrokkene is de mens over wie de persoonsgegevens gaan: in het po en s(v)o is dit de leerling, in het mbo de student. Maar het kan ook gaan over een medewerker van de school zoals de conciërge, OOP'er, docent of de directeur. Als de betrokken leerling jonger is dan 16 jaar, dan mogen volgens de wet alleen zijn wettelijke vertegenwoordigers (ouders) beslissen over de gegevens van de betrokkene, de leerling/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. Deze functionaris wordt ook wel Data Protection Officer (DPO) genoemd. 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 uitvoering van de Wbp en AVG, wordt in Nederland uitgeoefend door de Autoriteit Persoonsgegevens (afgekort tot AP).

3.2. Samenwerkingsverbanden

Het samenwerkingsverband heeft een eigen wettelijke taak namelijk: het realiseren van een samenhangend geheel van ondersteuningsvoorzieningen binnen en tussen de scholen zodat leerlingen een ononderbroken ontwikkelingsproces kunnen doormaken. Het samenwerkingsverband is gericht op het geven van extra ondersteuning, door het bieden van extra ondersteuning krijgen leerlingen een zo passend mogelijke plaats in het onderwijs. Om te kunnen beoordelen welke extra ondersteuning nodig is, verwerkt het samenwerkingsverband gezondheidsgegevens van leerlingen. Die gezondheidsgegevens zijn 'bijzondere persoonsgegevens' en vereisen een zeer zorgvuldige omgang.

Het samenwerkingsverband is, ondanks dat de schoolbesturen *vertegenwoordigd* zijn in het samenwerkingsverband, een zelfstandige verwerkingsverantwoordelijke, zodat het bestuur daarvan, net als het bevoegd gezag, een FG moet aanwijzen.

3.3. Wie bepaalt of een FG aangewezen moet worden?

Het samenwerkingsverband is als verwerkingsverantwoordelijke eindverantwoordelijk voor privacy binnen de organisatie. Of een verwerkingsverantwoordelijke verplicht is een FG verplicht aan te wijzen, staat in de AVG.

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 dat organisaties meer toezicht en controle op de verwerking van persoonsgegevens krijgen. In eerdere teksten van de AVG (2015) was het alleen voor organisaties van een bepaalde grootte verplicht een FG aan te wijzen (bijvoorbeeld 250 werknemers of 5000 betrokkenen). In 2016 is er bewust voor gekozen om dit criterium uit de AVG te schrappen: een marketingbureau met 'slechts' 25 medewerkers kan meer 'gevoelige' persoonsgegevens verwerken dan een doorsnee bedrijf met 1000 werknemers. Mede daarom is overwogen dat de grootte van een organisatie geen goed criterium is. Om toch duidelijkheid te scheppen over de verplichting om een FG aan te stellen is in de uiteindelijke AVG is een functioneel criterium geïntroduceerd: niet de grote van de organisatie is bepalend maar de gevoeligheid van de verwerkingen zijn van belang voor het bepalen of het aanwijzen van een FG verplicht is (zie toelichting in paragraaf 3.5). Concrete criteria geeft de AVG niet, het is aan een organisatie zelf aan de hand van de AVG bepalen of een FG verplicht is.

Dit betekent dat *het bestuur* van het samenwerkingsverband formeel de keuze moet maken al dan niet een FG aan te stellen. Hiervoor is een gemotiveerd bestuursbesluit nodig. Kiest de bestuurder ervoor om geen FG aan te wijzen dan dient ook dit besluit te worden gemotiveerd. De toezichthouder, de Autoriteit Persoonsgegevens, kan achteraf toetsen of een FG aangewezen had moeten worden. Deze handreiking helpt samenwerkingsverbanden om *zelf* een afweging te maken of zij op grond van de AVG verplicht zijn een FG aan te wijzen.

Volgens de PO-Raad, VO-raad en Kennisnet is, gezien de wettelijke taak van het samenwerkingsverband en de gevoeligheid van de te verwerken persoonsgegevens door het samenwerkingsverband, het aanwijzen van een FG verplicht voor samenwerkingsverbanden.

3.4. Autoriteit Persoonsgegevens

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 scholen en samenwerkingsverbanden in heel Europa 'dus' een FG moeten hebben. De verwachting is niet dat de AP op korte termijn hier duidelijkheid over zal verschaffen.

Het is op dit moment ook nog niet duidelijk of de AP met regels komt 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.

3.5. Moet volgens de AVG een FG aangewezen worden?

Op basis van analyse van de wetgeving (die is opgenomen als bijlage 1) is de conclusie dat een samenwerkingsverband passend onderwijs - vanaf 25 mei 2018 – verplicht is een FG aan te wijzen op grond van de AVG, artikel 37 lid 1 sub a t/m c:

a) Het samenwerkingsverband 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;
b) Het samenwerkingsverband 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.
c) Het samenwerkingsverband *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*.

Uit deze analyse van de AVG volgt dat samenwerkingsverbanden een FG moeten aanwijzen. De PO-Raad, VO-raad en Kennisnet raden samenwerkingsverbanden aan dat te doen.

3.6. Wat als er op 25 mei 2018 nog geen FG is aangewezen?

De AVG verplicht samenwerkingsverbanden om een FG aan te wijzen. Volgens de strikte letter van de AVG moet dat op 25 mei 2018 geregeld zijn. Maar op die datum zullen nog niet alle samenwerkingsverbanden een FG hebben aangewezen. Daar is - meestal - een goede verklaring voor te geven.

Organisaties zijn druk bezig om informatiebeveiliging en privacy te regelen. Het aanwijzen van een FG is ‘slechts’ één van de vele zaken die geregeld moeten worden. Het verdient aanbeveling om eerst zaken te regelen zoals een informatiebeveiligings- en privacybeleid, het aanwijzen van één of meer medewerkers die zich bezighouden met de uitvoering van dit beleid, het organiseren van een risico-inventarisatie, het maken van een dataregister, een procedure ontwikkelen voor datalekken etc. Omdat een FG onafhankelijk toezicht moet houden, kan een FG zich niet tot in detail bezighouden met het organiseren en op orde krijgen van IBP: een FG kan natuurlijk pas toezicht houden als het beleid rondom IBP al geregeld is. Het aanwijzen van een FG is daarom eerder het sluitstuk voor het regelen van IBP, dan een startpunt.

Voor samenwerkingsverbanden die op 25 mei 2018 nog geen FG hebben aangewezen, maar wel bezig zijn om IBP te regelen, is het advies om schriftelijk vast te leggen waarom ze (nog) geen FG hebben aangewezen en wat de planning is om wel aan die verplichting te gaan voldoen. Daarmee kan het samenwerkingsverband verantwoorden waarom er nog niet aan de letter van de AVG wordt voldaan, en dat er hard gewerkt wordt om aan álle verplichtingen van de AVG te gaan voldoen.

3.7. Uitzonderingen op wettelijke verplichting

Voor zeer kleine organisaties die slechts op zeer beperkte schaal persoonsgegevens verwerken, geldt de wettelijke verplichting om een FG aan te wijzen *mogelijk* niet. Omdat de grootte van organisatie van de Verwerkingsverantwoordelijke niet het toetsingscriterium is maar de gevoeligheid van de aard van de persoonsgegevens verwerkt worden, geldt deze uitzondering niet voor het samenwerkingsverband. Het samenwerkingsverband verwerkt immers altijd gevoelige persoonsgegevens.

4. Hoe regel je een FG?

Dit hoofdstuk beschrijft hoe je een FG aanwijst.

4.1. Aanwijzen FG

Omdat aan het aanwijzen van een FG in de AVG wettelijke eisen gesteld worden, kan er niet worden afgeweken van een formele aanwijzing. Het aanwijzen van een FG gebeurt bij besluit van het samenwerkingsverband, dat schriftelijk gemotiveerd is. Gelijktijdig met het aanwijzen van de FG kan een 'Regeling voor de taken en bevoegdheden FG' worden vastgesteld, een voorbeeld hiervan is opgenomen in bijlage 2.

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 FG). 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 samenwerkingsverband. Zorg dat de aangewezen FG een gesprekpartner is (wordt) voor bestuur, collega's maar ook voor leerlingen en ouders.

4.2. 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). Omdat een FG aan een aantal formele vereisten moet voldoen, en onafhankelijk en vrijelijk moet kunnen opereren, is de personele invulling van deze functie niet flexibel uitwisselbaar. De titel FG mag niet zomaar gebruikt worden: iemand die belast is met privacy binnen de organisatie kan zich niet plotseling 'FG' gaan (laten) noemen.

Het is mogelijk dat een medewerker die reeds in dienst is, wordt aangewezen als FG (en dus de functie van FG krijgt). Dit is uiteraard alleen mogelijk als deze medewerker vanuit een onafhankelijke positie de functie van FG kan uitoefenen (zie paragraaf 4.3).

Voor wat betreft de positionering van de FG binnen de organisatie, schrijft de AVG voor dat de FG rechtstreeks verslag uitbrengt aan de hoogste leidinggevende binnen de organisatie.

4.3. Onafhankelijk

Een FG moet onafhankelijk (kunnen) zijn. De FG is immers niet alleen adviseur maar ook (intern) controleur. De onafhankelijkheid is geborgd in de wet, door bijvoorbeeld de wettelijke ontslagbescherming van een FG. Deze vereiste onafhankelijkheid maakt dat niet iedereen FG kan worden: een bestuurder, directeur of manager zal lastig FG kunnen worden, dit zou betekenen dat de FG-bestuurder zijn eigen werk moet gaan controleren. Maar ook het aanwijzen van een beleidsmedewerker ligt minder voor de hand: die is in de dagelijkse praktijk betrokken bij de besluitvorming over persoonsgegevens en kan daarom lastig(er) onafhankelijk toezicht houden. We kan de functie van FG goed gecombineerd worden met andere controlerende functies zoals die van een controller.

Overigens blijkt in de praktijk dat de 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 formeel onafhankelijk is, maar zich dus ook vrij voelt om onafhankelijk te opereren en adviseren.

4.4. Bekend maken aanwijzen FG

De AVG vereist dat het bestuur de contactgegevens van de FG publiceert en deze gegevens doorgeeft aan de relevante toezichthouder (zie 4.5.1.). De contactgegevens dienen informatie te bevatten die iedereen, binnen en

buiten organisatie en de toezichthouder in staat stellen de FG gemakkelijk en vertrouwelijk te bereiken. Te denken valt aan het vermelden van het postadres, een speciaal (rechtstreeks) 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. Bijzonderheid is dat de *naam* van de FG niet hoeft te worden vermeld (maar dat is soms wel praktischer).
Het is aan te raden de contractgegevens van de FG op te nemen op de website van het samenwerkingsverband.

4.5. Autoriteit Persoonsgegevens

Het is de bedoeling dat zich tussen de FG en de AP, een “soepel samenspel” ontwikkelt. De FG is geen verlengde arm van de AP: de FG is dan ook niet verplicht om de AP uit eigen beweging informatie te verstrekken. De FG moet gezien worden als eerstelijnstoezichthouder en die als intermediair kan 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 ook toezicht op organisaties of zij de functie van FG naar behoren hebben ingericht, en of deze functie in de praktijk ook goed wordt uitgevoerd.

4.5.1. Aanmelding FG

De Autoriteit Persoonsgegevens houdt een register bij van alle aangewezen FG’s. Het samenwerkingsverband is verplicht de 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://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/aanmelding_fg.pdf

De FG wordt opgenomen in het register van FG’s: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming/register-fg-a-tm-d

4.6. Externe FG

Het is overigens niet vereist dat een FG in loondienst is bij het samenwerkingsverband. De AVG biedt ook de mogelijkheid om een externe FG aan te wijzen. De FG wordt voor een aantal uur (per week of maand) 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, scholen en ouders/leerlingen (alle betrokkenen). De toezichthouder eist dat een FG betrokken is bij de organisatie waarvoor hij werkzaam is, dit kan niet als een FG slechts enkele dagen per jaar langs komt of contact heeft. Het is dan ook verstandig om regelmatig contact te hebben en de FG minstens maandelijks langs te laten komen.

Ook kan een FG worden aangewezen die werkzaam is bij een verwerker (leverancier). Belangrijk hierbij is wel dat een belangenconflict vermeden wordt en dat de FG onafhankelijk zijn werk kan doen. De verdeling van taken en verantwoordelijkheden moet daarom contractueel worden geregeld. Voor het samenwerkingsverband wordt deze mogelijkheid vanwege de verschillende belangen, niet aangeraden.

4.7. Samenwerking tussen samenwerkingsverbanden

De AVG biedt ook de mogelijkheid dat verwerkingsverantwoordelijken (samenwerkingsverbanden) samenwerken en gezamenlijk één of meerdere FG’s aanwijzen. Ook hierbij is het belangrijk dat deze FG vanuit elke organisatie 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 samenwerkingsverband 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 organisaties duidelijk te verdelen en voor elk bestuur één persoon als hoofdcontactpersoon (coördinator) aan te

wijzen. Denk hierbij aan de mogelijkheid om per samenwerkingsverband iemand aan te wijzen met privacy in het aandachtsgebied (bijvoorbeeld als privacy officer, zie paragraaf 4.9).

Een ander alternatief is samen met één of meerdere schoolbesturen een FG regelen. Juist omdat schoolbesturen in een regio samenwerken in het kader van passend onderwijs (waar bij uitstek veel bijzondere persoonsgegevens worden verwerkt), is een samenwerking met het samenwerkingsverband een goede mogelijkheid om gezamenlijk een FG te regelen.

4.8. MR

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.
Dit betekent dat de instemming van de Medezeggenschapsraad (MR) van het samenwerkingsverband vereist is voor het aanwijzen van een 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 MR 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. Indien het samenwerkingsverband geen MR heeft kan deze toetsing (hoewel niet formeel) door de Ondersteuningsplanraad (OPR) worden verricht.

Anders dan bij een onderwijsinstelling heeft de MR of OPR van het samenwerkingsverband heeft de MR van het samenwerkingsverband geen instemmings- of adviesrecht in het geval van vaststelling of wijziging van een regeling over het verwerken van en de bescherming van persoonsgegevens van de leerlingen. De MR of OPR van het samenwerkingsverband heeft alleen in geval van vaststelling of wijziging van een regeling over het verwerken van en de bescherming van persoonsgegevens van medewerkers van het samenwerkingsverband advies- of instemmingsrecht.

Omdat het in de praktijk voor een FG niet mogelijk is om bij de uitvoering van diens taken onderscheid te maken tussen leerling- of medewekersgegevens wordt geadviseerd om de regeling ten aanzien van de FG integraal voor te leggen aan de MR of, (mocht het samenwerkingsverband geen MR hebben) aan de OPR van het samenwerkingsverband.

.

4.9. Aansprakelijkheid

De AVG maakt in artikel 24 lid 1 duidelijk dat het niet de FG, maar de verwerkingsverantwoordelijke (het samenwerkingsverband) 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 (de AVG) wordt uitgevoerd”. Het feit dat de FG erop toeziet dat de AVG wordt nageleefd, wil dus niet zeggen dat de FG persoonlijk verantwoordelijk is wanneer dit niet het geval is. De werkgever blijft dan ook *verantwoordelijk* en *aansprakelijk* voor het werk dat een werknemer, zoals een FG, uitvoert. In het geval dat er gebruik wordt gemaakt van een externe FG, is het verstandig om aanvullend afspraken te maken over aansprakelijkheid en om zo nodig/gewenst een verzekering af te sluiten. Wie draait er bijvoorbeeld op voor de boete van de toezichthouder als de externe FG zijn taken niet naar behoren verricht?

5. Taken en bevoegdheden FG

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

5.1. 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 de:
   a. AVG,
   b. andere Unierechtelijke (lees: Europese) of nationale gegevensbeschermingsbepalingen, en
   c. van het beleid van het bestuur met betrekking tot de bescherming van persoonsgegevens (inclusief van verantwoordelijkheden, bewustmaking en opleiding van de medewerkers, en de betreffende audits).

   De AVG spreekt erover dat de FG het bestuur 'bijstaat bij het toezicht op de interne naleving van de AVG'.
3. 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 de *Aanpak IBP* voor een toelichting hierop). Om dit goed uit te voeren, kunnen FG's onder andere:
   a. informatie verzamelen om het (type) gebruik van persoonsgegevens te identificeren;
   b. analyseren en controleren in hoeverre het gebruik van persoonsgegevens aan de AVG voldoet; en
   c. het bestuur informeren, adviseren of aanbevelingen geven.
4. 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.
5. 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.

De FG mag naast zijn functie, ook andere taken uitvoeren, onder de voorwaarde dat die taken of plichten niet tot een belangenconflict leiden. De onafhankelijkheid van de FG is erg belangrijk (zie ook paragraaf 4.3).

5.2. 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". 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 het samenwerkingsverband gegevens verwerken.

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

- Nodig de FG regelmatig uit voor 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 leerlingen en medewerkers.
- Leg het schriftelijk vast als de adviezen van de FG 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).

5.2.1. Onafhankelijkheid

De FG mag geen belemmerende instructies ontvangen die ervoor zorgen dat de FG zijn taken en verplichtingen niet onafhankelijk kan vervullen. Ook mag het bestuur de 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.
Het is niet wenselijk dan een bestuurder ook FD is, 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. Het kan verstandig zijn om interne regels op te stellen om belangenconflicten te vermijden, of te bepalen welke taken de FG niet mag uitvoeren.

5.3. 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 op peil te houden. De FG moet bij zijn werk actief ondersteund worden door het management van het samenwerkingsverband.

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.

6. Expertise, functie-eisen en rechtspositie FG

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

6.1. 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).

Een FG hoeft niet persé een juridische opleiding, achtergrond of ervaring te hebben (al heeft dat wel de voorkeur). Uit de praktijk blijkt dat een IT-beheerder of ICT-coördinator ook ruime ervaring heeft met ICT en het verwerken van persoonsgegevens. Er zijn verschillende opleidingsmogelijkheden voor FG's om zich verder te scholen en bekwamen als deskundige.

Uit overweging 97 van de AVG wordt duidelijk een FG geen super-expert hoeft te zijn. De deskundigheid die nodig is wordt namelijk mede bepaald op grond van het gebruik van persoonsgegevens binnen de organisatie. Het vereiste kennisniveau moet passen bij de gevoeligheid, complexiteit en de hoeveelheid gegevens die binnen het samenwerkingsverband worden verwerkt. Een FG binnen een samenwerkingsverband zal gezien de gevoeligheid van de door het samenwerkingsverband verwerkte persoonsgegevens over meer kennis en expertise moeten beschikken dan een FG werkt bij een bestuur met (alleen) reguliere scholen onder zich. Over het algemeen geldt dat hoe complexer en/of gevoeliger de verwerkingen zijn, des te deskundiger de FG moet zijn.

6.2. 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);
- de wettelijke context van passend onderwijs kennen (weten wat de wettelijke taken zijn van het samenwerkingsverband en welke privacyregels daarbij van toepassing zijn);
- vaardigheden hebben om binnen de organisatie een cultuur van gegevensbescherming te ontwikkelen.

6.3. Ontslagbescherming

Om ervoor te zorgen dat de FG onafhankelijk kan opereren, geniet de FG op grond van artikel 38 lid 2 AVG ontslagbescherming. Het bestuur kan en mag een FG niet ontslaan omdat deze kritische adviezen geeft, of omdat deze het in uitvoering van zijn taak 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 een ondernemingsraad. Uiteraard is het wel toegestaan een FG te ontslaan indien deze niet functioneert of contractuele dan wel arbeidsrechtelijke instructies overtreedt.

7. Best practices

Dit hoofdstuk beschrijft op welke manieren er een FG kan worden aangewezen

7.1. Zelf een FG aanwijzen

Een samenwerkingsverband kan een externe FG aanwijzen (inhuren) en die wegwijs maken in de organisatie of een (interne) medewerker aanwijzen als FG en die op (laten) leiden tot FG. In beide gevallen geldt dat de FG niet fulltime hoeft te werken, maar ook bijvoorbeeld 1 dag per week als FG kan werken.

De FG moet beschikken over de nodige (juridische) expertise over privacy, moet de weg weten te vinden binnen de organisatie en 'het onderwijs' kennen. Omdat ieder samenwerkingsverband zijn eigen organisatiestructuur, procedures en afspraken heeft, leeft de ervaring dat zelfs een reeds bekwame FG van buiten het onderwijs, ook tijd nodig heeft om de taal van het onderwijs te leren spreken.

Het is belangrijk om te beseffen dat bij het inhuren van een externe FG, de eist blijft staan dat de FG betrokken is bij besluitvorming rondom privacy binnen het samenwerkingsverband. Wil een FG zijn werk goed kunnen doen, dan moet deze regelmatig geïnformeerd worden over het reilen en zeilen van het samenwerkingsverband. Ook moet de FG worden geconsulteerd bij vraagstukken rondom privacy. Daarbij lijkt een betrokkenheid van minstens één dag per maand het minimale.

7.2. Gezamenlijk een FG aanwijzen

Het is mogelijk dat een aantal samenwerkingsverbanden besluiten om gezamenlijk een FG aan te wijzen. Dit kan een extern ingehuurde FG zijn of een medewerker van een van de samenwerkingsverbanden of een van deelnemende schoolbesturen die wordt opgeleid tot FG. Belangrijk is dat één van de samenwerkingsverbanden de FG aanstuurt: die sluit het contract met de externe FG of stuurt de medewerker die FG is aan. De samenwerkende organisaties maken afspraken over de werkzaamheden, taken en verantwoordelijkheden van de FG. Onderdeel van de afspraken is dan ook de verrekening van de kosten van deze FG.

Bij het gezamenlijk aanwijzen van een FG, kan ook gedacht worden aan binnen het samenwerkingsverband met meerdere schoolbesturen waarbij meerdere schoolbesturen en het samenwerkingsverband gezamenlijk een FG benoemen. Omdat er bij het samenwerkingsverband alleen maar met bijzondere persoonsgegevens wordt gewerkt, zal er binnen deze organisatie meer expertise over privacy aanwezig (moeten) zijn. Ook in dit geval moeten de samenwerkende besturen afspraken maken over de taken en verantwoordelijkheden van deze FG.

7.3. Tijdbesteding

De omvang van de taken van een FG is sterk afhankelijk van de organisatie van het samenwerkingsverband. Voor een samenwerkingsverband met een goed georganiseerde staf en/of gespecialiseerde IT-medewerkers, waar het IBP-beleid al helemaal is doorgevoerd, is het eenvoudig voor een FG om de organisatie te leren kennen. Een samenwerkingsverband waarbij IBP nog in de kinderschoenen staat, zal zelf nog meer tijd nodig hebben om IBP goed te regelen. De FG zal dan ook meer tijd nodig hebben voor het begeleiden van de medewerkers die IBP gaan organiseren.

Na het aanwijzen van een (interne of externe) FG, zal de FG in het begin tijd kwijt zijn om de organisatie te leren kennen en om afspraken te maken met het bestuur en de medewerkers die betrokken zijn bij IBP.
Er is ook een verschil of er een externe ervaren FG wordt ingehuurd, of dat een interne medewerker FG is. Zoals in paragraaf 7.1 is gemeld, zal de FG toch maandelijks contact moeten of langs moeten gaan om te weten wat er speelt rondom IBP. Zonder regelmatig overleg en contact, kan de FG zijn functie niet vervullen zoals dat voorzien is in de wet.

Bijlage 1: Juridische onderbouwing aanwijzen FG

Deze bijlage geeft de juridische onderbouwing waarom een samenwerkingsverband passend onderwijs een FG moet aanwijzen.

1.1. Artikel 37 AVG

Of een samenwerkingsverband een FG moet aanwijzen, wordt bepaald aan de hand van 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 samenwerkingsverband een FG moet aanwijzen, zijn er uit de AVG de volgende criteria te destilleren:

a) Het samenwerkingsverband (= de verwerkingsverantwoordelijke) is aan te merken als *overheidsinstantie of overheidsorgaan*
b) *hoofdzakelijk belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen* vereisen
c) het samenwerkingsverband *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 specifiek gesproken over onderwijsinstellingen of samenwerkingsverbanden passend onderwijs, laat staan of de organisaties een FG moeten aanwijzen. Dat betekent dat uit de AVG zelf moet worden afgeleid of een FG verplicht is voor organisaties als samenwerkingsverbanden.

Deze verduidelijking wordt gegeven door de Artikel 29 werkgroep (Workingparty 29; WP29, vanaf 25 mei 2018 het 'Europees Comité voor gegevensbescherming'). Deze werkgroep bestaat uit vertegenwoordigers van alle toezichthouders. Het Comité zorgt ervoor dat de AVG consequent wordt toegepast en uitgelegd. Dat doen zij onder andere door het uitvaardigen van richtlijnen. Op 5 april 2017 zijn de "Richtlijnen voor functionarissen voor de gegevensbescherming"[1] vastgesteld. Deze richtlijn wordt hierna "Richtlijn FG's" genoemd en geeft meer informatie over de rol en (verplichte) aanstelling van een FG.

Volledigheidshalve moet worden vermeld dat, zelfs wanneer het niet verplicht is om een FG aan te wijzen, altijd *vrijwillig* een FG kan worden aangewezen. Er is overigens geen verschil tussen de rechten en verplichtingen van een vrijwillig of een verplicht aangestelde FG.

1.2. Het samenwerkingsverband als overheidsinstantie of overheidsorgaan

In Nederland is de vrijheid van onderwijs geregeld in de Grondwet. Nederland neemt hiermee een redelijk unieke positie in binnen Europa in. Onderwijs is in andere Europese landen doorgaans meer georganiseerd door overheden of vanuit overheidswege, waardoor scholen en daarmee samenhangende instanties sneller gezien worden als overheidsinstanties (art. 37 lid 1 sub a AVG).

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 aan de hand van Europese en Nederlandse wet- en regelgeving worden bepaald. In het Nederlands recht kan daarvoor worden gekeken naar het begrip 'bestuursorgaan' uit de Algemene wet bestuursrecht (Awb). Bepalend is of een organisatie zoals een school of een samenwerkingsverband een publieke taak vervult of met publiek gezag is omkleed. Het kan dus ook gaan om private organisaties die (voor een deel) een publieke taken uitvoeren.

In Nederland valt het openbaar onderwijs onder de Awb, het bijzonder onderwijs valt niet onder de Awb. Samenwerkingsverbanden zijn geen overheidslichamen maar privaatrechtelijk georganiseerd (in vereniging of stichting) en hebben een publieke taak. Wel worden samenwerkingsverbanden voor het afgeven van toelaatbaarheidsverklaringen (tlv's) gezien als bestuursorgaan in de zin van de Awb en is beroep mogelijk bij de bestuursrecht tegen tlv-beschikkingen. Samenwerkingsverbanden kunnen dus worden gezien als semi-overheid: een organisatie die 'dicht tegen de overheid aan zit'. Samenwerkingsverbanden hebben wettelijke taken en ze dienen het algemeen publiek belang, daarnaast zijn ze publiek gefinancierd. Het publiek belang bestaat uit het bieden van een passende plek in het onderwijs voor ieder kind en het zorgdragen voor een dekkend netwerk van ondersteuningsvoorzieningen.

Samenwerkingsverbanden worden in veel gevallen gelijk gesteld aan publiekrechtelijke instellingen. Zo zijn ze volgens de Aanbestedingswet aanbestedingsplichtig: een verplichting die alleen geldt publiekrechtelijke instellingen die een specifiek doel hebben om ten aanzien van het algemeen belang (anders dan van industriële of commerciële aard), die rechtspersoonlijkheid bezitten 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.

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

[1] Officieel (Guidelines on Data Protection Officers ('DPOs')) 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

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.

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, voeren deze 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: betrokkenen hebben doorgaan geen keus om hun persoonsgegevens te laten verwerken want er is meestal wetgeving die verplicht om deze persoonsgegevens 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.
Op basis van het bovenstaande is de conclusie gerechtvaardigd dat samenwerkingsverbanden onder de definitie van publiekrechtelijke instelling kunnen vallen: overheidsinstantie of –orgaan. Hoewel samenwerkingsverbanden privaatrechtelijk zijn georganiseerd vervullen zijn een publieke, wettelijke taak.

1.3. 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 samenwerkingsverbanden onder deze bepaling vallen.

1.3.1. 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 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, en zeker voor het samenwerkingsverband, treffend. De kerntaak van het samenwerkingsverband is het realiseren van een samenhangend geheel van ondersteuningsvoorzieningen binnen en tussen de scholen zodat dat leerlingen een ononderbroken ontwikkelingsproces kunnen doormaken. Voor het uitvoeren van deze taak is het noodzakelijk om

persoonsgegevens vast te leggen. In veel gevallen zullen dat gezondheids-, en dus bijzondere, persoonsgegevens zijn: zonder deze gegevens kan het samenwerkingsverband haar taak niet uitvoeren.

1.3.2. Aard, omvang en/of doeleinden van de verwerking van persoonsgegevens

In het kader van passend onderwijs worden er veel gegevens van en over leerlingen verwerkt. Op basis van deze gegevens kan het samenwerkingsverband beoordelen of een leerling toegelaten wordt tot speciaal onderwijs of adviseren over de ondersteuningsbehoefte van de leerling. 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;

1.3.3. 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:

a) het aantal betrokkenen – in specifieke cijfers of als percentage van de betreffende bevolking;
b) de hoeveelheid gegevens en/of de hoeveelheid verschillende gegevens die wordt verwerkt;
c) de duur of permanentie van de gegevensverwerking;
d) de geografische reikwijdte van de verwerking.

Grootschalig beoordelen in een kwantitatief perspectief, is lastig. Terwijl de grootste samenwerkingsverbanden (met meer dan honderd aangesloten scholen) persoonsgegevens verwerken van honderden leerlingen, zijn die persoonsgegevens inhoudelijk niet anders of minder gevoelig dan bij een klein samenwerkingsverband dat 'slechts' de persoonsgegevens van enkele tientallen leerlingen verwerkt. Daarnaast moet worden opgemerkt dat bijna de gehele verwerking van de samenwerkingsverbanden bestaat uit bijzondere persoonsgegevens van (vaak jonge en dus kwetsbare) leerlingen.

Een beter aanknopingspunt zijn de *duur*, *hoeveelheid* en *verscheidenheid* in gegevens die worden verwerkt. Gedurende de gehele schoolloopbaan worden er van leerlingen die ondersteuning van het samenwerkingsverband nodig hebben persoonsgegevens, verzameld, vastgelegd, beoordeeld en uitgewisseld. De Autoriteit Persoonsgegevens noemt in haar onderzoeksrapport naar Snappet[2] de door Snappet verzamelde gegevens van leerlingen "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. Samenwerkingsverbanden beschikken in hun administraties ook al over veel meer informatie over sociaal-emotionele ontwikkeling of gezondheidsgegevens (passend onderwijs). Daarmee kan snel worden aangenomen dat samenwerkingsverbanden beschikken over grote verzamelingen van gevoelige en bijzondere persoonsgegevens, waaraan allerlei conclusies verbonden kunnen worden die van grote invloed zijn op de privacy van de betrokken leerlingen.

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 individuele 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').

[2] https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013_snappet.pdf

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.

1.3.4. 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 leerlingadministratie- of leerlingvolgsysteem), 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 uitvoeren van de wettelijke taak van het samenwerkingsverband. In het kader van een tlv-aanvraag stuurt de school aan het samenwerkingsverband veelal het opgestelde Ontwikkelingsperspectief (OPP) mee of werkt met het zgn. groei-document. Onderdeel daarvan is monitoringgegevens over de leerling, de ingezette acties van de school en de resultaten daarvan. De school moet aan het samenwerkingsverband aantoonbaar maken dat zij niet de juiste ondersteuning kunnen bieden; dit is niet mogelijk zonder gegevens te overleggen over een langere periode van de leerling waaruit blijkt wat de school heeft gedaan en wat de resultaten waren ten aanzien van de leerling waar een tlv voor wordt gevraagd.

Het bieden van een passende onderwijsplek door het samenwerkingsverband zonder te beschikken over gegevens met betrekking tot het monitoren en observeren van leerlingen is niet mogelijk. Daarmee wordt voldaan aan dit criterium.

1.4. 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 zoals het samenwerkingsverband 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 tot en met 1.3.3 van deze bijlage.

Bij deze categorie verwerkingen gaat het om het gebruik van bijzondere persoonsgegevens (deze worden beschreven in artikel 9 AVG). Indien instellingen zich dus veel bezig houden met bijzondere persoonsgegevens zoals gezondheidsgegevens, moeten zij een FG aanwijzen. Dit is in het bijzonder het geval bij het samenwerkingsverband: het samenwerkingsverband beoordeeld leerlingdossiers waarin veel bijzondere persoonsgegevens van (voornamelijk) sociaal-emotionele of gezondheidsaard zijn opgenomen. Samenwerkingsverbanden hebben van al deze leerlingen een dossier met zeer gevoelige persoonsgegevens die grote invloed hebben op de privacy. Daarom is het aanwijzen van een FG noodzakelijk volgens de AVG.

1.5. Moet volgens de wet een FG aangewezen worden?

Op basis van een analyse van de wetgeving is de conclusie dat een samenwerkingsverband - vanaf 25 mei 2018 een FG dient aan te wijzen op grond van de AVG, artikel 37 lid 1 sub:

a) Het samenwerkingsverband is aan te merken als of gelijk te stellen aan een *overheidsinstantie of overheidsorgaan;*
b) Het samenwerkingsverband 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.

c) Het samenwerkingsverband *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*.

1.6. Uitzondering: geen FG aanwijzen

Het samenwerkingsverband moet zelf beoordelen of zij onder de hiervoor beschreven criteria vallen. Alhoewel het dringende advies is om wel een FG aan te wijzen, kan een samenwerkingsverband 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 moet aanwijzen.

Het is mogelijk dat de in de AVG genoemde criteria in de toekomst worden verduidelijkt, bijvoorbeeld door een nieuwe Richtlijn FG's die exacte cijfers als criterium geeft voor de hoeveelheid betrokkenen, medewerkers of persoonsgegevens 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.

Ook als het samenwerkingsverband van mening is dat de AVG het aanstellen van een FG niet specifiek verplicht stelt, kan het voor het bestuur zinvol zijn vrijwillig een FG aan te wijzen. In de Richtlijn FG's moedigt de Artikel 29-werkgroep 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 samenwerkingsverbanden (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 Wbp en is aangepast aan de terminologie van de AVG.

DE GEEL GEARCEERDE TEKST MOET INGEVULD WORDEN

Regeling taken en verantwoordelijkheden Functionaris voor Gegevensbescherming

Artikel 1: definities

a. AVG: Algemene Verordening Gegevensbescherming;
b. FG: functionaris voor gegevensbescherming artikel 37 van de AVG;
c. Verwerkingsverantwoordelijke: het bestuur van [naam samenwerkingsverband]
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:
    a. het houden van toezicht op verwerkingen van persoonsgegevens;
    b. toezicht op wijzigingen in bestaande verwerkingen en/of het aanleggen van nieuwe verwerkingen met persoonsgegevens binnen [naam samenwerkingsverband];
    c. geven van (ongevraagd) advies en doen van aanbevelingen over privacy in het algemeen en de toepassing van de AVG;
    d. overleg met (de contactpersoon van) de Autoriteit Persoonsgegevens;
    e. Organiseren, inrichten en/of onderhouden van het verwerkingsregister (dataregister) met alle verwerkingen persoonsgegevens binnen [naam samenwerkingsverband];
    f. *OPTIONEEL*: jaarlijks opstellen van een verslag van zijn werkzaamheden;
    g. het (laten) afhandelen van klachten inzake privacy;
    h. Overige door het bestuur of directie van [naam samenwerkingsverband] aan de FG opgedragen werkzaamheden aangaande privacy.
2. Het personeel meldt bij de FG alle (nieuwe) verwerkingen van persoonsgegevens alsmede eventuele incidenten met betrekking tot privacy.
3. *OPTIONEEL*: De security officer is betrokken bij de dagelijkse operationele gang van zaken met betrekking tot de diensten en voorzieningen van [naam samenwerkingsverband]. De security officer overlegt met en informeert de FG terzake van privacygerelateerde kwesties en vraagstukken over de voorzieningen van [naam samenwerkingsverband].

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 [naam samenwerkingsverband] 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 [naam samenwerkingsverband] werkzaam is of overeenkomstig voor of namens [naam samenwerkingsverband] 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 de duur van maximaal één werkdag mee te nemen.
6. De FG is bevoegd tot het geven van een opdracht tot
    a. het aanmaken van een registratie van persoonsgegevens in overeenstemming met de AVG;
    b. 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 [naam samenwerkingsverband], 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 [naam samenwerkingsverband] 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.

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 bestuur van [naam samenwerkingsverband] 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.

DE GEEL GEARCEERDE TEKST MOET INGEVULD WORDEN

Voor samenwerkingsverband naam samenwerkingsverband ***zijn we op zoek naar een functionaris voor gegevensbescherming (FG) voor XX uur per week.***

Functiebeschrijving

CONTEXT
De werkzaamheden worden verricht binnen (naam samenwerkingsverband en omschrijving). De FG adviseert en rapporteert aan de directeur of directeur-bestuurder binnen het samenwerkingsverband.

Naam samenwerkingsverband treeft 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 samenwerkingsverband, is onafhankelijk en houdt toezicht op de toepassing en naleving van privacywetgeving zoals de Algemene Verordening Gegevensverwerking die sinds 25 mei 2018 van kracht is. 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 directeur;
   - Maakt afwijkingen van voorgenoemde voorschriften en regelingen bespreekbaar en maakt afspraken met de verantwoordelijke functionaris;
   - Adviseert en ondersteunt onderdelen van het samenwerkingsverband 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 Algemene Verordening Gegevensbescherming (AVG)
   - Levert een bijdrage aan het ontwerpen, 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;
   - Leidt of neemt deel aan overlegvormen, projecten en samenwerkingsverbanden op het gebied van de informatiebeveiliging en privacy;
   - Fungeert als (eerste) aanspreekpunt voor zaken betreffende de AVG binnen de organisatie;
   - 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 zorgt voor een passend niveau van beveiliging van de informatiehuishouding;
   - Neemt maatregelen gericht op het beperken van (het gebruik van) persoonsgegevens.
   - Houdt een bestand van verwerkingen van persoonsgegevens (dataregister) bij;
   - 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 organisatie 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 uit.
   - 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 Wet Bescherming Persoonsgegevens.

KADER, BEVOEGDHEDEN EN VERANTWOORDELIJKHEDEN

Verantwoording schuldig aan:
de directeur of directeur-bestuurder van het samenwerkingsverband 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.
- Algemeen theoretische en praktische kennis van (Informatie)beveiliging en privacy wetgeving.
- Kennis van en inzicht in de taak- en doelstelling en de werkwijze van de organisatie van het samenwerkingsverband.
- Inzicht in de bedrijfs- en onderwijsprocessen binnen het samenwerkingsverband.
- 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 de aangesloten schoolbesturen van het samenwerkingsverband om met uiteenlopende belangen om te gaan, informatie te geven en de uitvoering af te stemmen;
- Met de directeur en het bestuur van het samenwerkingsverband om informatie te geven en de naleving van de AVG af te stemmen;
- Met de directeur 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 directeur 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.

Bijlage 4:

Informatiebeveiligings- en privacybeleid (IBP)

voor het Samenwerkingsverband

Versie 1.4
26 maart 2018

Voorwoord

Digitalisering in de maatschappij leidt tot toenemende beschikbaarheid van data en potentieel dus tot nieuwe of rijkere informatie. Digitalisering speelt ook een grote rol binnen het onderwijs, datasturing en informatisering maken het mogelijk om steeds beter samen te werken.

Digitalisering brengt ook risico's met zich mee. Het leidt tot vraagstukken rondom het verzamelen van data en de verschillende vormen van classificatie daarbinnen. Denk daarbij in het bijzonder aan persoonsgegevens. Met welk doel worden ze verzameld, wie beslist hierover, wie heeft ervoor getekend? En indien je met de juiste doelbinding beschikt over data hoe ga je er dan qua beveiliging mee om, zodat je voorkomt dat ze in verkeerde handen kunnen vallen.

Het samenwerkingsverband ondersteunt scholen bij het aanbieden van passend onderwijs. Omdat we daarbij met gevoelige persoonsgegevens omgaan, moet informatiebeveiliging en privacy voor ons natuurlijk op orde zijn. In dit document laten wij zien aan iedereen met wij samenwerken, intern en extern, hoe wij dat georganiseerd hebben.

Voor het samenwerkingsverband zijn Informatiebeveiliging en privacy onlosmakelijk met elkaar verbonden en integraal onderdeel van beleid, processen en uitvoering. We hebben gekozen voor ISO 27001 als verzameling van beveiligingsmaatregelen om ons continue proces van risicoafweging en mitigerende maatregelen vorm te geven. Verder gelden security en privacy by design. Dit zorgt er ook voor dat IBP geen papieren tijger is of wordt maar een onderdeel van onze dagelijkse werkwijze.

<>

Bestuurder samenwerkingsverband

1. Het belang van informatiebeveiliging en privacy

Uitwisselen van bijzondere persoonsgegevens is onderdeel van het dagelijks werk in het samenwerkingsverband. Hierbij hebben we te maken met een groot aantal mogelijke bedreigingen. Alle systemen die we gebruiken en gegevens die we bewaren en verwerken, kunnen worden bedreigd door bijvoorbeeld een aanval, een vergissing of de natuur (zoals een overstroming of brand).

Datalekken, incorrecte gegevens of diensten die niet beschikbaar zijn - in het ergste geval schaden deze incidenten onze bedrijfsvoering en daarmee het vertrouwen. Daarom zijn de continuïteit van onze dienstverlening en privacybescherming van groot belang. Ook treffen we gericht maatregelen om mogelijke risico's tot een aanvaardbaar niveau te reduceren.

Het bestuur doet daarom een beroep op iedereen die betrokken is bij de activiteiten van het samenwerkingsverband, vanuit een gemeenschappelijke visie en wil, de verwerking van (persoons)gegevens correct te laten verlopen.

Dit beleid gaat dieper in op de bescherming van ict en in het bijzonder persoonsgegevens. Het dient als norm en leidraad voor alle informatieverwerking en biedt een uitgangspunt voor audit en controle.

Dit beleid biedt elke belanghebbende – medewerker, klant of leverancier – een inzage in de manier waarop we omgaan met persoonsgegevens.

1.7. De scope van het informatiebeveiligings- en privacybeleid

Het informatiebeveiligings- en privacybeleid is van toepassing op alle informatieverwerking binnen en namens het samenwerkingsverband.

Het beleid is van toepassing op onze eigen medewerkers, tijdelijk personeel en op personeel dat door derden wordt ingezet om diensten te verlenen aan of namens onze organisatie.

1.8. Het doel van informatiebeveiliging en privacy

Het Informatiebeveiligings- en privacybeleid heeft de volgende doelen:

- Het waarborgen van de continuïteit van de dienstverlening;
- Het beschermen van de privacy van eenieder van wie het samenwerkingsverband persoonsgegevens verwerkt;
- Het voorkomen en zo goed mogelijk afhandelen van incidenten;
- Het minimaliseren van de eventuele gevolgen van incidenten.

Bij het realiseren van deze doelen bewaakt het samenwerkingsverband de balans tussen werkbaarheid – in de meest brede zin van het woord – en informatiebeveiliging en privacy.

2. Het beleid

Het beleid bestaat uit keuzes die het samenwerkingsverband maakt om de doelen rond informatiebeveiliging en privacy te bereiken.

2.1. Voorbeeldrol

Het samenwerkingsverband heeft een voorbeeldrol in de onderwijsketen en communiceert helder en actief over informatiebeveiliging en privacy. Alle medewerkers en diensten van het samenwerkingsverband dienen voorbeeldig te zijn wat betreft informatiebeveiliging en privacy.

2.2. Wet- en regelgeving

Het samenwerkingsverband houdt zich aan alle relevante wet- en regelgeving. Twee regels vormen daarbij de basis:

- De bestuurder van het samenwerkingsverband is eindverantwoordelijk voor de bescherming van persoonsgegevens.
- Het samenwerkingsverband hanteert passende technische en organisatorische maatregelen voor het beschermen van diensten en in het bijzonder persoonsgegevens.

2.3. IBP is overal in verweven

Het samenwerkingsverband beschouwt informatiebeveiliging en privacy als onlosmakelijk met elkaar verbonden en als belangrijk onderdeel van het beleid, de processen en de uitvoering van diensten. Daar waar mogelijk wordt informatiebeveiliging en privacy opgenomen in bestaande processen.

2.4. IBP is de verantwoordelijkheid van iedereen

Omdat iedereen binnen en rondom het samenwerkingsverband bijdraagt aan informatiebeveiliging en privacy, zijn de rollen en verantwoordelijkheden rondom informatiebeveiliging en privacy duidelijk vastgelegd.

2.5. ISO 27001 als basis

Het samenwerkingsverband kiest ISO 27001 (en ISO 27002) als een verzameling van geschikte beveiligingsmaatregelen. Hierbij is het proces voor informatiebeveiliging doorlopend en cyclisch. Dat betekent dat het samenwerkingsverband jaarlijks de organisatie als geheel evalueert, controleert en verbetert. Nieuwe ontwikkelingen of incidenten, binnen en buiten het samenwerkingsverband, aanschaf van diensten of bedrijfsmiddelen en grote wijzigingen in de dienstverlening zijn aanleiding tot extra valuatie, controle en eventuele bijstelling.

Het samenwerkingsverband past classificatie, privacy by design, security by design en privacy by default toe om passende maatregelen te kunnen treffen.

3. Uitvoering

Om het informatiebeveiligings- en privacybeleid te realiseren, besteedt het samenwerkingsverband aandacht aan een aantal zaken.

3.1. Bewustzijn

Het bevorderen van bewustzijn rondom informatiebeveiliging en privacy is de verantwoordelijkheid van alle medewerkers. Het beveiligingsbewustzijn wordt vergroot door:

- Voorlichting (security awareness training)
- Opstellen en uitdragen van gedragsregels (handleiding aanvaardbaar gebruik bedrijfsmiddelen)

Deze middelen dragen het volgende uit:

- Het belang van informatiebeveiliging en privacy voor Het samenwerkingsverband
- Nieuwe ontwikkelingen op het gebied van informatiebeveiliging en privacy (bijvoorbeeld actuele incidenten)
- De belangrijkste veiligheidsmaatregelen rond dagelijkse werkzaamheden
- Waar mensen terecht kunnen bij incidenten of met ideeën en vragen

3.2. Incidenten en datalekken

Medewerkers die een incident of inbreuk rond informatiebeveiliging en/of privacy vermoeden, dienen dit te melden. Een vraag of suggestie over informatiebeveiliging en privacy kan ook als incident gemeld worden. Alle meldingen worden volgens een vast proces behandeld.

Een interne medewerker kan melding doen bij de Servicedesk of via email naar security@hetsamenwerkingsverband.nl. Wanneer het om persoonsgegevens gaat, wordt de Functionaris voor de Gegevensbescherming (FG) ingeschakeld. Na afhandeling van het incident wordt de melder ingelicht over de afhandeling daarvan.

Een melding van incidenten of verzoeken rondom persoonsgegevens door externe partijen kan gedaan worden bij de Servicedesk, of via email naar support@hetsamenwerkingsverband.nl. Op de website van het samenwerekingsverband, staat deze loketfunctie vermeld. Externe partijen en betrokkene kunnen bij dit loket terecht voor:

- Algemene informatie over de verwerking van persoonsgegevens.
- Verzoeken voor inzage van de eigen verwerkte persoonsgegevens en eventuele wijziging of verwijdering daarvan.

3.3. Naleving

Schending van de wetgeving, voorschriften of regels rond informatiebeveiliging en privacy kan leiden tot corrigerende maatregelen zoals non-actiefstelling, disciplinaire straffen en beëindiging van een contract of dienstverband.

3.4. Actualiteit

Het samenwerkingsverband houdt rekening met actuele ontwikkelingen. Daarom wordt dit beleid minimaal elke twee jaar getoetst en bijgesteld door het managementteam (MT) aan de hand van het volgende:

- De behoeften en verwachtingen van belanghebbenden in de onderwijsketen
- De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's)
- De effectiviteit van de genomen maatregelen en aantoonbare werking daarvan
- Wet- en regelgeving

3.5. Wet- en regelgeving

Het samenwerkingsverband voldoet aan alle wet- en regelgeving die relevant is in dit verband zoals maar niet beperkt tot:

- De Algemene Verordening Gegevensbescherming;
- De Archiefwet – in het bijzonder bewaartermijnen;
- Het Privacyconvenant;
- Etc, etc.

Ter uitvoering van de privacyregels heeft het samenwerkingsverband een privacyreglement vastgesteld[3]

3.6. De vijf vuistregels van privacy

Het samenwerkingsverband houdt zich bij het verwerken van persoonsgegevens aan de beginselen rond de verwerking persoonsgegevens (art.5 AVG). De vijf vuistregels van privacy zijn:

1. Doelbepaling en doelbinding: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt voor andere doeleinden.
2. Grondslag: verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen.
3. Dataminimalisatie: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt. Het type persoonsgegevens staat in verhouding tot het doel – het doel kan niet met minder of alternatieve gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. Transparantie: het samenwerkingsverband legt aan betrokkenen (zoals leerlingen, hun ouders en medewerkers) op transparante manier en ongevraagd verantwoording af over het gebruik van hun persoonsgegevens en het beleid daarover. Daarnaast hebben de betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Ook kunnen betrokkenen zich geheel verzetten tegen het gebruik van hun persoonsgegevens.
5. Data-integriteit: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

3.7. Dataregister

Alle verwerkingen binnen en namens het samenwerkingsverband worden vastgelegd en up-to-date gehouden in een dataregister.

3.8. Planning & controle

Het samenwerkingsverband doorloopt een jaarlijkse planning- en controlecyclus voor informatiebeveiliging en privacy, deze bestaat minimaal uit de volgende activiteiten:

- Risico-inventarisatie en selectie van maatregelen.
  In het eerste kwartaal van elk jaar vindt een risicoworkshop plaats om de grootste risico's te identificeren. De resultaten hiervan bepalen welke informatiebeveiligingsmaatregelen geïmplementeerd of verbeterd dienen te worden in dat jaar.
- Controle en rapportage
  Operationele controle op de naleving van beleid en richtlijnen wordt verricht door het lijnmanagement. De <rol bestuurslid> rapporteert elk kwartaal aan het bestuur over de informatiebeveiliging binnen het samenwerkingsverband, de vorderingen rond implementatie en verbetering van maatregelen en de incidenten in dat kwartaal. Aan het einde van het jaar rapporteert de <rol bestuurslid> over de implementatie van informatiebeveiligingsmaatregelen die uit de risicoworkshop zijn gekomen.
- Interne audit
  Controle op de implementatie en borging van het informatiebeveiligings- en privacybeleid en de richtlijnen en maatregelen die hieruit voortkomen. Deze vindt gedurende het jaar plaats en wordt gedetailleerd beschreven in het 'Handboek interne audit informatiebeveiliging en privacy'. De uitkomst van deze audit wordt gerapporteerd aan de <rol bestuurslid>.
- Externe audit
  Minimaal jaarlijks vindt een onafhankelijke controle van de informatiebeveiliging van één of meerdere onderdelen van de primaire bedrijfsvoering van het samenwerkingsverband plaats. De uitkomst van deze audit wordt gerapporteerd aan het bestuur.

Zie model: [3] http://steunpuntpassendonderwijs-vo.nl/nieuw-privacyreglement/

4. Organisatie

Het samenwerkingsverband verdeelt de rollen en verantwoordelijkheden voor informatiebeveiliging en privacy als volgt:

4.1. Medewerkers

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden, zoals beschreven in het Personeelshandboek en de 'Handleiding acceptabel gebruikmaken van bedrijfsmiddelen'. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

Wij vragen medewerkers zich actief bezig te houden met informatiebeveiliging. Bijvoorbeeld door meldingen te maken van security incidenten, verbetervoorstellen te doen en invloed uit te oefenen op het beleid binnen het samenwerkingsverband.

4.2. Management

De bestuurder is de eindverantwoordelijke voor informatiebeveiliging en privacy.

Het bestuur is verantwoordelijk voor:

- Het vaststellen van het informatiebeveiligingsbeleid en de daaruit volgende richtlijnen voor Het samenwerkingsverband.
- Het evalueren van de toepassing en werking van het informatiebeveiligings-beleid op basis van rapportages.

Binnen het bestuur is <rol bestuurslid> portefeuillehouder voor informatiebeveiliging en privacy.

Het lijnmanagement:

- Ziet toe op de naleving van het informatiebeveiligings- en privacybeleid door medewerkers.
- Heeft een positieve en actieve houding ten aanzien van informatiebeveiliging en privacy.
- Fungeert als voorbeeldfunctie.
- Behandelt informatiebeveiliging in bijvoorbeeld werkoverleg en beoordelingen.
- Handelt vertrouwelijke informatiebeveiligingsincidenten af.

4.3. Specifieke verantwoordelijkheden (ter voorbeeld)

Voor de uitvoering van het informatiebeveiligings- en privacybeleid zijn onder meer nodig: beleidsvoorbereiding, beheer van de processen, richtlijnen en procedures en controle op de naleving daarvan. Het samenwerkingsverband verdeelt deze verantwoordelijkheden als volgt:

- De (functie invullen) houdt de centrale geautomatiseerde informatievoorziening en de beveiliging daarvan in stand.
- De functie invullen) is het technische aanspreekpunt rond informatiebeveiliging binnen het samenwerkingsverband.
- De functie invullen) beheert het personeelsbeleid van het samenwerkingsverband. Dit raakt de informatiebeveiliging en privacy wat betreft de selectie, de voorlichting en het ontslag van personeel en het gebruik en delen van personeelsgegevens.
- De functie invullen) is verantwoordelijk voor de huisvesting. Binnen informatiebeveiliging is vooral de fysieke beveiliging van het kantoorpand een belangrijk thema.
- De functie invullen) is verantwoordelijk voor de informatiebeveiliging rond administratieve procedures.
- De Functionaris voor de Gegevensbescherming (FG) houdt toezicht op de naleving van de Wet bescherming persoonsgegevens binnen het samenwerkingsverband. Hij of zij doet aanbevelingen voor een betere bescherming van persoonsgegevens. De FG meldt voorgenomen verwerking van persoonsgegevens, indien nodig, aan de toezichthouder.
- De (functie invullen) beheert het loket voor inzageverzoeken en meldingen van externe partijen.