AUTORITEIT
PERSOONSGEGEVENS

Richtlijnen voor functionarissen voor de gegevensbescherming (FG's)

Deze tekst is een onofficiële Nederlandse vertaling van Guidelines on Data Protection Officers ('DPOs') van de Artikel 29-werkgroep van Europese privacytoezichthouders. De vertaling is gemaakt in opdracht van de Autoriteit Persoonsgegevens en is daarom niet wettelijk bindend. Mocht de Nederlandse vertaling afwijken van de originele Engelse tekst, dan is de Engelse tekst leidend.

Inhoudsopgave

1. Inleiding

De algemene verordening gegevensbescherming (AVG)[1], die op 25 mei 2018 ingaat, biedt een gemoderniseerd, op verantwoording gebaseerd kader voor de naleving van regels op het gebied van gegevensbescherming in Europa. Functionarissen voor de gegevensbescherming (FG's) zullen in dit nieuwe juridische kader voor veel organisaties centraal staan en naleving van de bepalingen van de AVG mogelijk maken.

Onder de AVG zijn bepaalde verantwoordelijken en verwerkers verplicht een FG aan te wijzen.[2] Dit geldt voor overheidsinstanties en -organen (ongeacht de door hen verwerkte gegevens) en voor andere organisaties die – als een van hun kerntaken – stelselmatig en op grote schaal personen observeren of op grote schaal bepaalde categorieën persoonsgegevens verwerken.

Ook waar de AVG het aanstellen van een FG niet specifiek verplicht stelt, kan het voor sommige organisaties zinvol zijn vrijwillig een FG aan te wijzen. De Artikel 29-werkgroep van Europese privacytoezichthouders (WP29) moedigt deze vrijwillige initiatieven aan.

Het idee van een FG is niet nieuw. Hoewel Richtlijn 95/46/EG[3] het aanwijzen van een FG niet verplicht stelt, is het in verschillende lidstaten in de afgelopen jaren toch de gewoonte geworden om een FG aan te wijzen.

Ook vóór de invoering van de AVG zag WP29 de FG al als een hoeksteen voor verantwoording en stelde WP29 dat het aanwijzen van een FG de naleving kan vergemakkelijken en daarnaast een concurrentievoordeel voor bedrijven kan vormen.[4] Naast het mogelijk maken van naleving door het invoeren van verantwoordingsinstrumenten (zoals het mogelijk maken of uitvoeren van *privacy impact assessments* en het uitvoeren van controles), fungeren FG's als tussenpersonen tussen de verschillende belanghebbenden (zoals toezichthouders, betrokkenen en bedrijfseenheden binnen een organisatie).

FG's zijn niet persoonlijk verantwoordelijk wanneer de AVG niet nageleefd wordt. De AVG maakt duidelijk dat het de verantwoordelijke of de verwerker is die erop toe dient te zien en moet kunnen aantonen dat de verwerking aan de voorwaarden voldoet (Artikel 24(1)). Naleving van regels op het gebied van gegevensbescherming is de verantwoordelijkheid van de verantwoordelijke of de verwerker.

---

[1] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), (OJ L 119, 4.5.2016).

[2] Het aanwijzen van een FG is tevens verplicht voor bevoegde instanties onder Artikel 32 van Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (OJ L 119, 4.5.2016, p. 89-131), en nationale implementatiewetgeving. Deze richtlijnen zijn weliswaar op FG's onder de AVG gericht, maar zijn wat betreft de vergelijkbare bepalingen tevens relevant voor FG's onder Richtlijn 2016/680.

[3] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (OJ L 281, 23.11.1995, p. 31).

[4] Zie: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

Daarnaast speelt de verantwoordelijke of de verwerker een cruciale rol in het mogelijk maken van een effectieve uitoefening van de taken van de FG. Het aanwijzen van een FG is een goede eerste stap, maar FG's dienen ook voldoende autonomie en middelen te hebben om hun taken goed uit te kunnen oefenen.

De AVG erkent dat de FG een sleutelfiguur is om ervoor te zorgen dat organisaties voldoen aan het nieuwe wettelijk kader en bevat regels voor zijn aanwijzing, positie en taken. Het doel van deze richtlijnen is het verduidelijken van de relevante voorwaarden van de AVG om verantwoordelijken en verwerkers te helpen aan de wet te voldoen, maar ook om FG's in hun functie te helpen. De richtlijnen bevatten tevens aanbevelingen (*good practices*) op basis van in bepaalde EU-lidstaten opgedane ervaring. WP29 houdt toezicht op de invoering van deze richtlijnen en kan deze waar nodig met verdere details aanvullen.

2. Aanwijzing van een FG

2.1 Verplichte aanwijzing

Onder Artikel 37(1) van de AVG is in drie specifieke gevallen het aanwijzen van een FG verplicht[5]:

a) wanneer de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan[6];
b) wanneer de verantwoordelijke of de verwerker hoofdzakelijk verwerkingen uitvoert die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen; of
c) wanneer de verantwoordelijke of de verwerker hoofdzakelijk grootschalige verwerkingen uitvoert van bijzondere categorieën van gegevens[7] of[8] persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten.[9]

In de volgende paragrafen biedt WP29 informatie over de criteria en de terminologie in Artikel 37(1).

Tenzij duidelijk is dat een organisatie niet verplicht is een FG aan te wijzen, raadt WP29 verantwoordelijken en verwerkers aan de uitgevoerde interne analyse vast te leggen om te bepalen of er al of niet een FG aangewezen moet worden, om aan te kunnen tonen dat met de betreffende factoren goed rekening is gehouden.[10]

Wanneer een organisatie vrijwillig een FG aanwijst, gelden voor zijn aanwijzing, positie en taken dezelfde voorwaarden van Artikel 37 tot en met 39 die zouden gelden als de aanwijzing verplicht was geweest.

Dit betekent niet dat een organisatie die niet vrijwillig een FG wil aanwijzen en daar niet wettelijk toe verplicht is, niet toch werknemers of externe adviseurs mag aanstellen met taken op het gebied van de

[5] Let op: onder Artikel 37(4) kan volgens wetgeving van de EU of de lidstaat het aanwijzen van FG's in andere situaties ook verplicht zijn.
[6] Met uitzondering van rechtbanken die in die hoedanigheid handelen.
[7] Onder Artikel 9 zijn dit onder andere persoonsgegevens waaruit iemands raciale of etnische achtergrond, politieke opvattingen, geloofsovertuiging of filosofische opvattingen of een lidmaatschap van een vakbond blijkt, en het verwerken van genetische gegevens, biometrische gegevens met het doel een natuurlijke persoon te identificeren, gegevens over de gezondheid of gegevens over het seksleven of de geaardheid van een natuurlijke persoon.
[8] In Artikel 37(1)(c) wordt het woord 'en' gebruikt. Zie Sectie 2.1.5 hieronder voor een uitleg van het gebruik van 'of" in plaats van 'en'.
[9] Artikel 10.
[10] Zie Artikel 24(1).

bescherming van persoonsgegevens. In dat geval is het belangrijk erop toe te zien dat er geen verwarring bestaat over hun functie, status, positie en taken. Daarom moet in alle communicatie binnen het bedrijf, met gegevensbeschermingsinstanties, met de betrokkenen en met het publiek duidelijk gemaakt worden dat deze persoon of adviseur geen FG is.[11]

2.1.1 'Overheidsinstantie of -orgaan'

De AVG biedt geen definitie van een 'overheidsinstantie of -orgaan'. WP29 ziet dit als iets dat op grond van nationale wetgeving bepaald dient te worden. Daarom vallen onder de term 'overheidsinstanties en -organen' nationale, regionale en lokale instanties, maar in de toepasselijke nationale wetgeving valt daaronder doorgaans ook een scala aan publiekrechtelijke instanties.[12] In dergelijke gevallen is het aanwijzen van een FG verplicht.

Overheidstaken mogen worden uitgevoerd en publiek gezag mag worden uitgeoefend[13] door zowel overheidsinstanties of -organen als – uit hoofde van publiek recht of privaatrecht – door andere natuurlijke personen of rechtspersonen, in bijvoorbeeld (in overeenstemming met de nationale regelgeving van een lidstaat) het openbaar vervoer, water- en energievoorziening, infrastructuur, de publieke omroep, huisvesting of disciplinaire instanties voor beschermde beroepen.

In deze gevallen bevinden betrokkenen zich wellicht in vrijwel dezelfde situatie als diegenen wier gegevens door een overheidsinstantie of -orgaan verwerkt worden. Dit houdt met name in dat gegevens mogelijk voor soortgelijke doelen verwerkt worden, mensen in beide gevallen weinig of geen keuze hebben of en hoe hun gegevens worden verwerkt, en daarom wellicht dezelfde aanvullende bescherming nodig hebben die met de aanwijzing van een FG bereikt kan worden.

Hoewel in dergelijke gevallen geen verplichting bestaat, raadt WP29 als een good practice aan dat:

- privaatrechtelijke organisaties die overheidstaken verrichten of publiek gezag uitoefenen een FG aanwijzen en
- ook alle verrichte verwerkingen onder de verantwoordelijkheid van de FG komen te vallen, met inbegrip van die handelingen die geen verband houden met het uitvoeren van een overheidstaak of officiële verplichting (bijv. het beheer van een database van medewerkers).

2.1.2 'Kerntaken'

Artikel 37(1)(b) en (c) van de AVG verwijst naar de "kerntaken van de verantwoordelijke of de verwerker". Volgens overweging 97 hebben de kerntaken van een verantwoordelijke betrekking op "diens hoofdactiviteiten en niet op de verwerking van persoonsgegevens als nevenactiviteit". 'Kerntaken' zijn de belangrijkste handelingen die nodig zijn om het doel van de verantwoordelijke of de verwerker te bereiken.

[11] Dit is ook relevant voor *chief privacy officers* (CPO's) of andere privacydeskundigen die sommige bedrijven al in dienst hebben en die wellicht niet altijd aan de AVG-criteria voldoen, bijvoorbeeld op het gebied van de beschikbare middelen of de garantie van onafhankelijkheid, en derhalve niet als FG gezien mogen worden of zo genoemd mogen worden.
[12] Zie bijv. de definitie van 'openbaar lichaam' en 'publiekrechtelijke instelling' in Artikel 2(1) en (2) of Richtlijn 2003/98/EG van het Europese Parlement en de Raad van 17 november 2003 inzake het hergebruik van overheidsinformatie (OJ L 345, 31.12.2003, p. 90).
[13] Artikel 6(1)(e).

Dit betekent echter niet dat activiteiten waarbij de verwerking van gegevens een onlosmakelijk onderdeel van de werkzaamheden van een verantwoordelijke of verwerker zijn, geen kerntaken zijn. Zo is de kerntaak van een ziekenhuis het bieden van gezondheidszorg. Een ziekenhuis is echter niet in staat veilige en effectieve gezondheidszorg te bieden zonder medische gegevens, zoals de medische dossiers van patiënten, te verwerken. Daarom dient het verwerken van deze gegevens als een van de kerntaken van een ziekenhuis gezien te worden en moeten ziekenhuizen FG's aanwijzen.

Een ander voorbeeld is een beveiligingsbedrijf dat een aantal winkelcentra en openbare gelegenheden bewaakt. De kerntaak van het bedrijf is bewaking, wat onlosmakelijk is verbonden met het verwerken van persoonsgegevens. Derhalve dient ook dit bedrijf een FG aan te wijzen.

Aan de andere kant voeren alle organisaties bepaalde werkzaamheden uit, zoals het betalen van hun medewerkers en het bieden van standaard ICT-ondersteuning. Dit zijn noodzakelijke ondersteunende functies voor de kerntaak of belangrijkste activiteit van de organisatie. Hoewel deze werkzaamheden noodzakelijk of essentieel zijn, worden ze doorgaans als nevenactiviteit gezien en niet als kerntaak.

2.1.3 'Grote schaal'

Artikel 37(1)(b) en (c) stelt dat aanwijzing van een FG nodig is wanneer op grote schaal verwerking van persoonsgegevens plaatsvindt. De AVG verduidelijkt niet wat onder 'op grote schaal' verstaan wordt, maar overweging 91 geeft wel een idee hiervan.[14]

Het is ook niet mogelijk exacte cijfers te geven die in alle gevallen gelden voor de hoeveelheid gegevens die verwerkt zou moeten worden of het aantal betrokken personen. Dit sluit echter niet uit dat, in de loop der tijd, een standaard ontwikkeld kan worden voor het bepalen van objectieve, kwantitatieve criteria voor wat, met betrekking tot bepaalde, veelvoorkomende verwerkingsactiviteiten, als 'grootschalig' gezien wordt. WP29 is ook van plan aan deze ontwikkeling bij te dragen, door voorbeelden van ondergrenzen voor de aanwijzing van een FG te delen en publiceren.

In ieder geval raadt WP29 aan om bij de bepaling of verwerking op grote schaal plaatsvindt met name de volgende factoren mee te nemen:

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

[14] Volgens de overweging betreft dit met name "grootschalige verwerkingen die bedoeld zijn voor de verwerking van een aanzienlijke hoeveelheid persoonsgegevens op regionaal, nationaal of supranationaal niveau, waarvan een groot aantal betrokkenen gevolgen zou kunnen ondervinden en die bijvoorbeeld vanwege hun gevoelige aard een hoog risico met zich kunnen brengen". Aan de andere kant stelt de overweging nadrukkelijk dat "de verwerking van persoonsgegevens niet als een grootschalige verwerking mag worden beschouwd als het gaat om de verwerking van persoonsgegevens van patiënten of cliënten door een individuele arts, een andere zorgprofessional of door een advocaat". Hier dient opgemerkt te worden dat, hoewel de overweging voorbeelden biedt van de uitersten (verwerking door een individuele arts versus verwerking van gegevens van een heel land of heel Europa), er een groot grijs gebied tussen deze uitersten is. Daarnaast dient rekening gehouden te worden met het feit dat deze overweging betrekking heeft op een privacy impact assessment. Dit houdt in dat sommige elementen wellicht specifiek in dergelijke gevallen gelden en niet per definitie op precies dezelfde manier voor de aanwijzing van FG's.

Voorbeelden van verwerking op grote schaal:

- verwerking van patiëntgegevens als onderdeel van de gebruikelijke werkzaamheden van een ziekenhuis;
- verwerking van reisinformatie van mensen die met het openbaar vervoer in een bepaalde stad reizen (door deze bijv. te volgen via reiskaarten);
- het voor statistische doeleinden verwerken van actuele locatiegegevens van klanten van een internationale fastfoodketen, door een verwerker die in deze diensten gespecialiseerd is;
- verwerking van klantgegevens als onderdeel van de gebruikelijke werkzaamheden van een verzekeringsmaatschappij of bank;
- verwerking van persoonsgegevens door een zoekmachine voor het tonen van advertenties op basis van internetgedrag;
- verwerking van gegevens (inhoud, verkeer, locatie) door telefoon- of internetproviders.

Voorbeelden van verwerking die niet als verwerking op grote schaal gezien wordt:

- verwerking van patiëntgegevens door een individuele arts;
- verwerking van persoonsgegevens over veroordelingen en strafbare feiten door een individuele advocaat.

2.1.4 'Regelmatige en stelselmatige observatie'

De AVG biedt geen definitie van het begrip 'regelmatige en stelselmatige observatie van betrokkenen', maar in overweging 24[15] wordt over 'het monitoren van het gedrag van de betrokkenen' gesproken, waaronder duidelijk alle vormen van volgen en profilering op het internet worden verstaan, waaronder voor het tonen van advertenties op basis van internetgebruik.

Het idee van observatie is echter niet beperkt tot het internet en observatie van internetgedrag dient gezien te worden als slechts één voorbeeld van het monitoren van het gedrag van betrokkenen.[16]

Onder 'regelmatig' verstaat WP29 een of meerdere van de volgende voorbeelden:

- voortdurend of gedurende een bepaalde periode, met bepaalde tussenpozen;
- terugkerend of op vaste tijden herhaald;
- constant of periodiek.

Onder 'stelselmatig' verstaat WP29 een of meerdere van de volgende voorbeelden:

- op basis van een systeem;
- vooraf geregeld, georganiseerd of systematisch;

[15] "Om uit te maken of een verwerking kan worden beschouwd als monitoring van het gedrag van betrokkenen, dient te worden vastgesteld of natuurlijke personen op het internet worden gevolgd, en onder meer of in dat verband eventueel persoonsgegevensverwerkingstechnieken worden gebruikt waarbij een profiel wordt opgesteld van een natuurlijke persoon, in het bijzonder om besluiten over hem te nemen of om zijn persoonlijke voorkeuren, gedragingen en attitudes te analyseren of te voorspellen."

[16] Let op: overweging 24 heeft betrekking op extraterritoriale toepassing van de AVG. Daarnaast is er een verschil tussen de formulering 'het monitoren van hun gedrag' (Artikel 3(2)(b)) en 'regelmatige en stelselmatige observatie van betrokken' (Artikel 37(1)(b)) waardoor dit als twee verschillende dingen gezien kan worden.

- als onderdeel van een algemeen plan voor het verzamelen van gegevens;
- als onderdeel van een strategie.

Voorbeelden: het exploiteren van een telecommunicatienetwerk; het bieden van telecommunicatiediensten; e-mail *retargeting*; profilering en beoordeling voor risicoanalyse (bijv. voor kredietbeoordeling, het bepalen van verzekeringspremies, fraudepreventie, het detecteren van witwaspraktijken); lokalisering met bijvoorbeeld mobiele apps; klantenkaarten; advertenties op basis van internetgedrag; het controleren van het welzijn, de conditie en de gezondheid door draagbare apparaten; beveiligingscamera's; verbonden apparatuur zoals slimme meters, smart cars, smart homes enz.

2.1.5 Speciale categorieën gegevens en gegevens over veroordelingen en strafbare feiten

Artikel 37(1)(c) betreft de verwerking van bijzondere categorieën van gegevens onder Artikel 9 en van persoonsgegevens over veroordelingen en strafbare feiten als bedoeld in Artikel 10. Hoewel in de bepaling het woord 'en' gebruikt wordt, is het geen beleidsregel dat de twee criteria tegelijkertijd toegepast moeten worden. In deze tekst moet 'en' daarom opgevat worden als 'of'.

2.2 FG van de verwerker

Artikel 37 geldt voor de aanwijzing van een FG voor zowel verantwoordelijken[17] als voor verwerkers[18]. Afhankelijk van wie aan de vereisten voor verplichte aanwijzing voldoet, is in sommige gevallen alleen de verantwoordelijke of alleen de verwerker en zijn in andere gevallen zowel de verantwoordelijke als de verwerker verplicht een FG aan te wijzen (die vervolgens samen dienen te werken).

Het is belangrijk op te merken dat zelfs als de verantwoordelijke aan de vereisten voor verplichte aanwijzing voldoet, diens verwerker niet per definitie verplicht is een FG aan te wijzen. Dit kan echter een good practice zijn.

Voorbeelden:

- Een klein familiebedrijf dat zich bezighoudt met de distributie van huishoudelijke apparatuur binnen één stad maakt gebruik van de diensten van een verwerker die als kernactiviteit webanalysediensten biedt n hulp met op internetgedrag gebaseerde advertenties en marketing. Gezien het kleine aantal klanten en het relatief kleine aantal activiteiten gelden de activiteiten van het familiebedrijf en zijn klanten niet als het verwerken van gegevens op 'grote schaal'. De werkzaamheden van de verwerker, die veel klanten zoals deze kleine onderneming heeft, gelden echter wel als verwerking op grote schaal. De verwerker moet daarom onder Artikel 37(1)(b) wel een FG aanwijzen. Tegelijkertijd is het familiebedrijf zelf niet verplicht een FG aan te wijzen.
- Een middelgrote tegelfabrikant besteedt arbodiensten uit aan een externe verwerker, die een groot aantal soortgelijke klanten heeft. De verwerker moet onder Artikel 37(1)(c) een FG aanwijzen, mits de verwerking op grote schaal plaatsvindt. De fabrikant is echter niet per definitie verplicht een FG aan te wijzen.

[17] Volgens Artikel 4(7) is de verantwoordelijke een natuurlijke persoon of instantie die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
[18] De verwerker is volgens Artikel 4(8) de persoon of het orgaan die/dat voor de verantwoordelijke persoonsgegevens verwerkt.

WP29 raadt als good practice aan dat een door een verwerker aangewezen FG ook toezicht houdt op handelingen die door de organisatie van de verwerkers worden verricht wanneer deze zelf als verantwoordelijke optreedt (bijv. HR, IT, logistiek).

2.3 'Vanuit elke vestiging makkelijk te contacteren'

Onder Artikel 37(2) is het toegestaan dat een concern van ondernemingen een gezamenlijke FG aanwijst, mits deze "vanuit elke vestiging makkelijk te contacteren is". Die 'bereikbaarheid' verwijst naar de functie van de FG als contactpersoon voor betrokkenen[19] en de toezichthouder[20] maar ook intern, binnen de organisatie, aangezien een van de taken van de FG is om "de verantwoordelijke of de verwerker en de werknemers die verwerken, te informeren en adviseren over hun verplichtingen onder deze Verordening".[21]

Teneinde ervoor te zorgen dat de FG, of deze nu intern of extern is, bereikbaar is, is het belangrijk dat diens contactgegevens volgens de bepalingen van de AVG beschikbaar zijn.[22]

Hij of zij dient in staat te zijn efficiënt met betrokkenen[23] te communiceren en met de betreffende toezichthouders samen te werken[24]. Dit betekent dat deze communicatie plaats dient te vinden in de taal of talen die door de betreffende toezichthouders en de betreffende betrokkenen gesproken wordt/worden.

Volgens Artikel 37(3), mag, met inachtneming van hun organisatorische structuur en grootte, voor meerdere overheidsinstanties of -organen een gezamenlijke FG aangewezen worden. Hetzelfde geldt voor middelen en communicatie. Aangezien de FG voor verscheidene taken verantwoordelijk is, dient de verantwoordelijke erop toe te zien dat één FG deze goed kan uitvoeren, ondanks het feit dat deze voor verschillende openbare instanties en organen verantwoordelijk is.

Het is essentieel dat de FG persoonlijk beschikbaar is (ofwel fysiek, op dezelfde locatie als de medewerkers, ofwel via een hotline of andere beveiligd communicatiemiddel) zodat betrokkenen contact met de FG op kunnen nemen. Uit hoofde van het recht van de EU of lidstaten heeft de FG een geheimhoudings- of vertrouwelijkheidsplicht bij de uitoefening van zijn taken (Artikel 38(5)). De geheimhoudings- of vertrouwelijkheidsplicht betekent echter niet dat de FG geen contact op mag nemen of advies in mag winnen bij de toezichthouder.

[19] Artikel 38(4): "Betrokkenen kunnen met de functionaris voor de gegevensbescherming contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten onder deze verordening".
[20] Artikel 39(1)(e): "als contactpunt voor de toezichthouder inzake met verwerking verband houdende aangelegenheden, met inbegrip van de in artikel 36 bedoelde voorafgaande raadpleging, en, waar passend, overleg plegen over enige andere aangelegenheid".
[21] Artikel 39(1)(a).
[22] Zie ook Sectie 2.5 hieronder.
[23] Artikel 12(1): "De verantwoordelijke neemt passende maatregelen opdat de betrokkene de in de artikelen 13 en 14 bedoelde informatie en de in de artikelen 15 tot en met 22 en artikel 34 bedoelde communicatie in verband met de verwerking in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt, in het bijzonder wanneer de informatie specifiek voor een kind bestemd is."
[24] Artikel 39(1)(d): "met de toezichthouder samenwerken"

2.4 Deskundigheid en vaardigheden van de FG

Artikel 37(5) stelt dat de FG "wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de in artikel 39 bedoelde taken te vervullen". Overweging 97 stelt dat het vereiste niveau van deskundigheid met name dient te worden bepaald op grond van de uitgevoerde gegevensverwerkingen en de bescherming die voor de door de verantwoordelijke of de verwerker verwerkte gegevens vereist is.

Kennisniveau

Het vereiste kennisniveau is niet specifiek aangegeven, maar dient te passen bij de gevoeligheid, complexiteit en de hoeveelheid gegevens die een organisatie verwerkt. Als de gegevensverwerking bijvoorbeeld bijzonder complex is of het een grote hoeveelheid gevoelige informatie betreft, heeft de FG wellicht meer kennis en steun nodig. Daarnaast maakt het uit of de organisatie stelselmatig persoonlijke informatie naar buiten de EU verzendt of dat dit slechts sporadisch voorkomt. Derhalve dient de FG zorgvuldig gekozen te worden, rekening houdend met de gegevensbeschermingskwesties binnen de organisatie.

Professionele kwaliteiten

Hoewel Artikel 37(5) niet specifiek aangeeft welke professionele kwaliteiten bij de aanwijzing van de FG van belang zijn, is het belangrijk dat FG's bekend zijn met nationale en Europese gegevensbeschermingswetten en -gebruiken en dat zij diepgaande kennis van de AVG hebben. Daarnaast is het goed als de toezichthouders passende en regelmatige training van FG's aanmoedigen.

Kennis van de bedrijfstak en de organisatie van de verantwoordelijke is aan te raden. De FG dient voldoende inzicht te hebben in de uitgevoerde gegevensverwerkingen en de informatiesystemen en de behoeften van de verantwoordelijke op het gebied van veiligheid van gegevens en gegevensbescherming.

Indien het een overheidsinstantie of -orgaan betreft, dient de FG ook goede kennis van de administratieve regels en procedures van de organisatie te hebben.

Vermogen zijn taken te vervullen

Het vermogen de taken te vervullen die bij de positie van FG horen moet worden opgevat als persoonlijke kwaliteiten en kennis van de FG, maar heeft ook te maken met de positie van de FG binnen de organisatie. Belangrijke persoonlijke kwaliteiten zijn bijvoorbeeld integriteit en professionele ethiek; de belangrijkste taak van de FG is te zorgen dat de AVG nageleefd wordt. De FG speelt een belangrijke rol in het creëren van een gegevensbeschermingscultuur binnen de organisatie. Ook helpt de FG met de implementatie van essentiële elementen van de AVG, zoals de beginselen van gegevensverwerking[25], de rechten van de betrokkenen[26], *privacy by design* en *privacy by default*[27], de administratie van gegevensverwerkingen[28], beveiliging van het verwerkingsproces[29] en melding van en communicatie over datalekken[30].

[25] Hoofdstuk II.
[26] Hoofdstuk III.
[27] Artikel 25.
[28] Artikel 30.
[29] Artikel 32.
[30] Artikel 33 en 34.

FG op basis van een servicecontract

De functie van de FG kan ook vervuld worden op basis van een servicecontract met een natuurlijk persoon of organisatie buiten de organisatie van de verantwoordelijke/verwerker. In het laatste geval is het essentieel dat elk lid van de organisatie die de taken van een FG vervult aan alle relevante vereisten van Artikel 4 van de AVG voldoet (zo is het bijvoorbeeld essentieel dat niemand een belangenconflict heeft). Het is net zo belangrijk dat elk lid de bescherming van de bepalingen van de AVG geniet (bijvoorbeeld: geen oneerlijke beëindiging van een servicecontract voor het uitvoeren van de taken van de FG, maar ook geen oneerlijk ontslag van een lid van de organisatie die de taken van de FG uitvoert). Tegelijkertijd kunnen individuele vaardigheden en talenten worden gecombineerd, waardoor verschillende personen, als team, hun klanten wellicht efficiënter kunnen dienen.

Voor de juridische duidelijkheid en goede organisatie wordt aangeraden de taken binnen het FG-team duidelijk te verdelen en voor elke klant één persoon als hoofdcontactpersoon aan te wijzen en 'de leiding' te geven. Het is over het algemeen ook aan te raden dit in het servicecontract op te nemen.

2.5 Publicatie en communicatie van de contactgegevens van de FG

Artikel 37(7) van de AVG vereist dat de verantwoordelijke of de verwerker:

- de contactgegevens van de FG publiceert en
- de contactgegevens aan de relevante toezichthouders communiceert.

Het doel van deze vereisten is erop toe te zien dat betrokkenen (zowel binnen als buiten de organisatie) en de toezichthouders gemakkelijk, direct en vertrouwelijk contact met de FG op kunnen nemen zonder met een ander onderdeel van de organisatie contact te hoeven opnemen.

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

Artikel 37(7) vereist niet dat bij de gepubliceerde contactgegevens de naam van de FG vermeld wordt. Hoewel dit een good practice is, is het aan de verantwoordelijke en de FG om te bepalen of dit in de betreffende omstandigheden vereist of zinnig is.[31]

WP29 raadt als good practice aan dat een organisatie de toezichthouder en medewerkers de naam en contactgegevens van de FG geeft. Zo kunnen de naam en contactgegevens van de FG intern bijvoorbeeld op het intranet van de organisatie, in het interne telefoonboek en in organogrammen vermeld worden.

[31] Het is belangrijk op te merken dat, in tegenstelling tot Artikel 37(7), Artikel 33(3)(b) – waarin de in geval van een datalek aan de toezichthouder en de betrokkenen te leveren informatie beschreven staat – specifiek vereist dat de naam (en niet alleen de contactgegevens) van de FG wordt vermeld.

3. Positie van de FG

3.1 Betrokkenheid van de FG bij alle aangelegenheden die de bescherming van persoonsgegevens betreffen

Artikel 38 van de AVG vereist dat de verantwoordelijke en de verwerker erop toezien dat de FG "naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens".

Het is van cruciaal belang dat de FG zo vroeg mogelijk betrokken wordt bij alle aangelegenheden die de bescherming van persoonsgegevens betreffen. Wat betreft privacy impact assessments, stelt de AVG expliciet dat de FG daar in een vroeg stadium bij betrokken dient te worden en vereist de AVG dat de verantwoordelijke bij het uitvoeren van dergelijke privacy impact assessments het advies van de FG inwint.[32] Wanneer de FG direct geïnformeerd en geraadpleegd wordt, is het makkelijker de AVG na te leven en wordt privacy by design geboden. Daarom dient dit een standaardprocedure binnen de organisatie te zijn. Daarnaast is het belangrijk dat de FG als een gesprekspartner binnen de organisatie gezien wordt en dat hij of zij deel uitmaakt van de relevante werkgroepen die binnen de organisatie gegevens verwerken.

Daarom dient de organisatie er bijvoorbeeld op toe te zien dat:

- De FG regelmatig wordt uitgenodigd om aan vergaderingen van het hoger management en het middenmanagement deel te nemen.
- Er wordt aangeraden hem uit te nodigen wanneer beslissingen met gevolgen voor gegevensbescherming worden genomen. Alle relevante informatie dient tijdig aan de FG doorgegeven te worden om hem in staat te stellen passend advies te geven.
- Aan de mening van de FG dient altijd passende waarde gehecht te worden. Bij geschillen raadt WP29 aan om vast te leggen waarom het advies van de FG niet gevolgd is.
- De FG dient onmiddellijk geraadpleegd te worden indien zich een datalek of ander incident heeft voorgedaan.

Waar nodig kan de verantwoordelijke of verwerker gegevensbeschermingsrichtlijnen of -programma's opstellen waarin aangegeven staat wanneer de FG geraadpleegd dient te worden.

3.2 Benodigde middelen

Artikel 38(2) van de AVG vereist dat de organisatie haar FG ondersteunt door "door hem toegang te verschaffen tot persoonsgegevens en verwerkingen en door hem de benodigde middelen ter beschikking te stellen voor het vervullen van deze taken en het in stand houden van zijn deskundigheid". Met name het volgende dient hierbij te gelden:

- Actieve ondersteuning van de functie van de FG door het hogere management (bijv. op het niveau van het bestuur).

[32] Artikel 35(2).

- Voldoende tijd voor de FG om zijn taken te vervullen. Dit is vooral belangrijk wanneer de FG op parttimebasis aangewezen wordt en een medewerker de FG-taken naast zijn andere werkzaamheden uitvoert. Indien dit niet het geval is, kunnen belangenconflicten ertoe leiden dat taken van de FG verwaarloosd worden. Het is van essentieel belang dat er voldoende tijd is om aan de taken van de FG te besteden. Wanneer het geen fulltimepositie is, is het good practice om een percentage van de tijd voor de FG-functie te reserveren. Daarnaast is het good practice de tijd die nodig is om de functie te vervullen en de prioriteit van de FG-taken te bepalen en tot slot dat de FG (of de organisatie) een werkplan opstelt.
- Voldoende steun qua financiële middelen, infrastructuur (terrein, faciliteiten, apparatuur) en, waar nodig, personeel.
- Officiële communicatie over de aanwijzing van de FG naar alle medewerkers, zodat zijn bestaan en functie binnen de organisatie bekend is.
- De vereiste toegang tot andere diensten, zoals personeelszaken, de juridische afdeling, de ICT-afdeling, de beveiliging enz., zodat de FG van die andere afdelingen de essentiële steun, input en informatie ontvangt.
- Doorlopende training. FG's dienen de kans te krijgen bij te blijven op het gebied van gegevensbescherming. Het streven moet zijn het kennisniveau van de FG doorlopend te verhogen en hij moet aangemoedigd worden om aan trainingen over gegevensbescherming en andere vormen van professionele ontwikkeling deel te nemen, zoals deelname aan privacy-fora, workshops enz.
- Op basis van de grootte en structuur van de organisatie, kan het nodig zijn een FG-team aan te stellen (een FG en zijn personeel). In dergelijke gevallen dienen de interne structuur van het team en de taken en verantwoordelijkheden van elk lid duidelijk aangegeven te worden. Wanneer de taken van de FG door een externe dienstverlener vervuld worden, mag een team van werknemers van dat bedrijf de taken van een FG ook als team uitvoeren, onder leiding van een aangewezen hoofdcontactpersoon voor de klant.

Over het algemeen geldt dat hoe complexer en/of gevoeliger de verwerkingen zijn, hoe meer middelen de FG geboden dienen te worden. De gegevensbeschermingsfunctie dient met het oog op de gegevensverwerking voldoende effectief te zijn en voldoende middelen te hebben.

3.3 Instructies en 'onafhankelijk handelen'

Artikel 38(3) schrijft enkele basisgaranties voor die ervoor moeten zorgen dat FG's hun taken met voldoende autonomie binnen een organisatie kunnen uitvoeren. Dit betekent met name dat de verantwoordelijken/verwerkers verplicht zijn erop toe te zien dat de FG "geen instructies ontvangt met betrekking tot de uitvoering van [zijn] taken". Overweging 97 voegt hieraan toe dat FG's "in staat dienen te zijn hun taken en verplichtingen onafhankelijk te vervullen, ongeacht of zij in dienst zijn van de verantwoordelijke".

Dit betekent dat bij het vervullen van hun taken onder Artikel 39, FG's geen instructies over de behandeling van een zaak mogen ontvangen, bijvoorbeeld over het te bereiken resultaat, het onderzoeken van een klacht of het raadplegen van een toezichthouder. Verder mogen ze geen instructies ontvangen om een bepaald standpunt in te nemen over een gegevensbeschermingskwestie, bijvoorbeeld over de wettelijke interpretatie.

De autonomie van FG's houdt echter niet in dat hun beslissingsbevoegdheid verder gaat dan hun taken onder Artikel 39.

De verantwoordelijke of de verwerker blijft verantwoordelijk voor de naleving van de privacywetgeving en moet kunnen aantonen dat deze nageleefd wordt.[33] Indien de verantwoordelijke of verwerker beslissingen neemt die niet aan de AVG voldoen en die niet met het advies van de FG overeenkomen, dient de FG de gelegenheid geboden te worden zijn afwijkende mening duidelijk te maken aan diegenen die de beslissingen nemen.

3.4 Ontslag of sancties voor het uitvoeren van FG-taken

Artikel 38(3) vereist tevens dat een FG "niet ontslagen of gestraft wordt voor de uitvoering van zijn taken".

Dit vereiste versterkt tevens de autonomie van FG's en helpt ervoor te zorgen dat zij onafhankelijk handelen en bij hun taken voldoende bescherming genieten.

Sancties zijn onder de AVG alleen verboden als deze opgelegd worden omdat de FG zijn taken als FG uitvoert. Zo is het mogelijk dat een FG van mening is dat een bepaalde verwerking een groot risico met zich meebrengt en de verantwoordelijke of de verwerker adviseert een privacy impact assessment uit te voeren, maar de verantwoordelijke of de verwerker het niet met de beoordeling van de FG eens is. In een dergelijk geval mag de FG niet ontslagen worden voor het geven van dit advies.

Sancties kunnen een aantal vormen hebben en kunnen zowel direct als indirect zijn. Hieronder vallen bijvoorbeeld het uitblijven of uitstellen van promoties; het voorkómen van verdere carrièreontwikkeling; het onthouden van voordelen die andere medewerkers wel krijgen. Deze straffen hoeven niet daadwerkelijk opgelegd te worden; de dreiging alleen al is voldoende zolang ze gebruikt worden om de FG te straffen voor het uitvoeren van zijn FG-activiteiten.

Een FG kan wél rechtmatig ontslagen worden als hier andere redenen aan ten grondslag liggen dan het uitvoeren van zijn taken als FG en als dit op basis van een gebruikelijke beleidsregel is en uit hoofde van de toepasselijke nationale contractenwet, arbeidswet en het strafrecht dat ook voor elke andere medewerker of aannemer zou gelden (bijvoorbeeld in geval van diefstal, fysieke, psychologische of seksuele intimidatie of soortgelijke zware misdragingen).

In deze context dient opgemerkt te worden dat de AVG niet aangeeft hoe en wanneer een FG ontslagen of vervangen kan worden. Wel geldt dat hoe stabieler het contract van een FG is en hoe meer garanties tegen oneerlijk ontslag er bestaan, hoe meer deze in staat zal zijn onafhankelijk op te treden. Derhalve moedigt WP29 organisaties aan dit te bewerkstelligen.

3.5 Belangenconflicten

Onder Artikel 38(6) mogen FG's "andere taken en plichten vervullen". Wel is vereist dat de organisatie erop toeziet dat "deze taken of plichten niet tot een belangenconflict leiden".

[33] Artikel 5(2).

De afwezigheid van belangenconflicten is nauw verbonden met de verplichting onafhankelijk op te treden. Hoewel FG's andere functies mogen hebben, mogen ze alleen andere taken en verantwoordelijkheden opgelegd krijgen als deze niet tot een belangenconflict leiden. Dit houdt met name in dat de FG geen positie in de organisatie mag hebben die ertoe leidt dat hij het doel van en de middelen voor het verwerken van persoonsgegevens bepaalt. Gezien de specifieke organisatorische structuur van elke organisatie dient dit per geval bekeken te worden.[34]

Afhankelijk van de activiteiten, grootte en structuur van de organisatie, is het wellicht een good practice als verantwoordelijken of verwerkers:

- Bepalen welke posities niet compatibel zijn met de functie van FG.
- Interne regels opstellen om belangenconflicten te vermijden.
- Een meer algemene uitleg geven van belangenconflicten.
- Verklaren dat hun FG geen belangenconflict heeft, om bewustheid van dit vereiste te creëren;
- Waarborgen in de interne regels van de organisatie inbouwen en erop toezien dat de vacature voor de positie van FG of het servicecontract specifiek en gedetailleerd genoeg is om belangenconflicten te vermijden. In dit verband dient er ook aan gedacht te worden dat, afhankelijk van de vraag of de FG intern of extern gerekruteerd is, belangenconflicten verschillende vormen kunnen aannemen.

4. Taken van de FG

4.1 Toezicht op naleving van de AVG

Artikel 39(1)(b) draagt de FG onder andere op erop toe te zien dat de AVG nageleefd wordt. Overweging 97 geeft verder aan dat FG's "de verantwoordelijke of de verwerker dient bij te staan bij het toezicht op de interne naleving van deze Verordening".

Als onderdeel van deze verplichting erop toe te zien dat de AVG nageleefd wordt, kunnen FG's met name:

- informatie verzamelen om verwerkingswerkzaamheden te identificeren;
- analyseren en controleren in hoeverre verwerkingswerkzaamheden aan de AVG voldoen; en
- de verantwoordelijke of de verwerker informeren, adviseren of aanbevelingen geven.

Het feit dat hij erop moet toezien dat de AVG nageleefd wordt, wil niet zeggen dat hij persoonlijk verantwoordelijk is wanneer hier niet aan voldaan wordt. De AVG maakt duidelijk dat het niet de FG, maar de verantwoordelijke is die verplicht is "passende technische en organisatorische maatregelen te treffen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening

[34] Als vuistregel zijn posities in het hoofdmanagement (zoals bestuursvoorzitter, operationeel directeur, financieel directeur, medisch directeur, hoofd van de marketingafdeling, hoofd van personeelszaken of hoofd van de ICT-afdeling) conflicterende posities, maar ook andere rollen lager in de organisatorische structuur als dergelijke posities of rollen leiden tot het bepalen van het doel en de middelen voor gegevensverwerking).

wordt uitgevoerd" (Artikel 24(1)). Naleving van regels op het gebied van gegevensbescherming is een bedrijfsverantwoordelijkheid van de verantwoordelijke en niet van de FG.

4.2 De rol van de FG in een privacy impact assessment

Volgens Artikel 35(1) is het de taak van de verantwoordelijke en niet van de FG om, waar nodig, een privacy impact assessment (PIA) uit te voeren. De FG kan echter een heel belangrijke en nuttige rol spelen bij het helpen van de verantwoordelijke. Volgens de beginselen van privacy by design, vereist Artikel 35(2) specifiek dat de verantwoordelijke bij een PIA "het advies van de FG inwint". Daarnaast draagt Artikel 39(1)(c) de FG op om "desgevraagd advies over het privacy impact assessment te verstrekken en toe te zien op de uitvoering daarvan".

WP29 raadt de verantwoordelijke aan onder andere over de volgende zaken het advies van de FG in te winnen[35]:

- of er al of niet een PIA uitgevoerd moet worden;
- welke methodiek voor de PIA gebruikt moet worden;
- of de PIA intern uitgevoerd of uitbesteed moet worden;
- welke waarborgen (zoals technische en organisatorische maatregelen) ingebouwd moeten worden om eventuele risico's voor de rechten en belangen van de betrokkenen te beperken;
- of de PIA correct uitgevoerd is en de conclusies daaruit (de vraag of de verwerking door moet gaan en welke waarborgen er ingebouwd moeten worden) aan de AVG voldoen.

Indien de verantwoordelijke het niet met het advies van de FG eens is, dient in de documentatie van de PIA specifiek schriftelijk aangegeven te worden waarom het advies niet overgenomen is[36].

Verder raadt WP29 de verantwoordelijke aan om de specifieke taken van de FG en de reikwijdte daarvan duidelijk aan te geven, bijvoorbeeld in het contract van de FG maar ook in de aan medewerkers, het bestuur (en, waar nodig, andere belanghebbenden) verstrekte informatie, met name waar het gaat om het uitvoeren van een PIA.

4.3 Risicogebaseerde benadering

Artikel 39(2) stelt dat de FG "bij de uitvoering van zijn taken naar behoren rekening (houdt) met het aan verwerkingen verbonden risico en met de aard, de omvang, de context en de verwerkingsdoeleinden".

Dit artikel is gebaseerd op een algemene standaard en gezond verstand, wat voor vele aspecten van de dagelijkse werkzaamheden van de FG van belang kan zijn. In feite vereist het dat de FG's hun

[35] Artikel 39(1) noemt de taken van de FG en geeft aan dat de FG 'ten minste' de volgende taken dient te hebben. Derhalve staat niets de verantwoordelijke in de weg de FG andere taken op te leggen dan de specifiek in Artikel 39(1) genoemde taken of die taken nader te beschrijven.

[36] Artikel 24(1) stelt dat "rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen treft om te waarborgen **en te kunnen aantonen** dat de verwerking in overeenstemming met deze Verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd."

werkzaamheden vooropstellen en zich vooral richten op zaken die een hoger risico voor gegevensbescherming vormen. Dit betekent niet dat zij het toezicht op naleving bij gegevensverwerkingen met een relatief laag risico mogen verwaarlozen, maar ze dienen zich wel met name op de werkzaamheden met een hoger risico te concentreren.

Deze selectieve en pragmatische aanpak helpt FG's de verantwoordelijke te adviseren over de bij het uitvoeren van een PIA te gebruiken methode, de zaken die bij een intern of extern gegevensbeschermingsonderzoek onderzocht dienen te worden, de interne trainingen die aan de voor de verwerking verantwoordelijke medewerkers of directieleden gegeven dienen te worden en aan welke verwerkingen hij meer tijd en middelen moet besteden.

4.4 De rol van de FG in het voeren van een administratie

Volgens Artikel 30(1) en (2), is het niet de FG, maar de verantwoordelijke respectievelijk de verwerker die verplicht is "een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden" of "een register van alle categorieën van verwerkingsactiviteiten die zij voor een verantwoordelijke hebben verricht" bij te houden.

In de praktijk maken FG's vaak inventarissen en houden een register van verwerkingen bij op basis van informatie die ze ontvangen van de verschillende organisaties die zich met het verwerken van persoonsgegevens bezighouden. Dit gebruik is in veel van huidige nationale wetten en onder de gegevensverwerkingsregels van EU-instanties en -lichamen vastgelegd.[37]

Artikel 39(1) bevat een lijst van taken die de FG ten minste moet hebben. Derhalve staat niets de verantwoordelijke of de verwerker in de weg om de FG de taak op te leggen om op verantwoordelijkheid van de verantwoordelijke het register van de verwerkingen bij te houden. Een dergelijk register dient gezien te worden als een van de middelen die de FG in staat stelt zijn taak te vervullen om op naleving toe te zien en de verantwoordelijke of de verwerker te informeren en adviseren.

In elk geval dient het register dat onder Artikel 30 bijgehouden dient te worden ook gezien te worden als een middel dat de verantwoordelijke en de toezichthouder, op verzoek, een overzicht biedt van alle verwerkingen van persoonsgegevens die een organisatie uitvoert. Derhalve is het een randvoorwaarde voor naleving en is het als zodanig een passend verantwoordingsmiddel.

[37] Artikel 24(1)(d), Verordening (EG) 45/2001.

AUTORITEIT
PERSOONSGEGEVENS

Contactgegevens

Bezoekadres

(alleen volgens afspraak)
Bezuidenhoutseweg 30
2594 AV DEN HAAG

Let op: bij bezoek aan de Autoriteit Persoonsgegevens moet u een geldig identiteitsbewijs laten zien.

Postadres

Postbus 93374
2509 AJ DEN HAAG

Telefonisch spreekuur

Op onze website autoriteitpersoonsgegevens.nl vindt u informatie en antwoorden op vragen over de bescherming van persoonsgegevens. Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met de publieksvoorlichters van de Autoriteit Persoonsgegevens tijdens het telefonisch spreekuur via telefoonnummer **0900-2001 201**. De publieksvoorlichters zijn bereikbaar op maandag, dinsdag, donderdag en vrijdag van 10.00 tot 12.00 uur. (5 cent per minuut, plus de kosten voor het gebruik van uw mobiele of vaste telefoon).

Persvoorlichting

Journalisten en redacteuren kunnen met vragen terecht bij de woordvoerders van de Autoriteit Persoonsgegevens via telefoonnummer **070-8888 555**.

Zakelijke relaties

Bent u een zakelijke relatie van de Autoriteit Persoonsgegevens, zoals een leverancier, dan kunt u ons telefonisch bereiken via telefoonnummer **070-8888 500**.

Over de Autoriteit Persoonsgegevens
Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.