GROEP GEGEVENSBESCHERMING ARTIKEL 29

16/NL
WP 243 rev.01

Richtlijnen voor functionarissen voor gegevensbescherming (Data Protection Officer, DPO)

Goedgekeurd op 13 december 2016

Laatstelijk herzien en goedgekeurd op 5 april 2017

DE WERKGROEP VOOR DE BESCHERMING VAN NATUURLIJKE PERSONEN IN VERBAND MET DE VERWERKING VAN PERSOONSGEGEVENS

Ingesteld bij Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995,

Gezien de artikelen 29 en 30,

Gezien het reglement van orde van de werkgroep,

HEEFT DE VOLGENDE RICHTLIJNEN VASTGESTELD:

Inhoudsopgave

1 Inleiding

De algemene verordening gegevensbescherming,[1] die op 25 mei 2018 van kracht wordt, biedt een gemoderniseerd, op verantwoording gebaseerd kader voor de naleving van regels inzake gegevensbescherming in Europa. Functionarissen voor gegevensbescherming zullen in dit nieuwe juridische kader voor veel organisaties centraal staan om naleving van de bepalingen van de algemene verordening gegevensbescherming mogelijk te maken.

Krachtens de algemene verordening gegevensbescherming moeten bepaalde verwerkingsverantwoordelijken en verwerkers een functionaris voor gegevensbescherming aanduiden[2]. Dit geldt voor alle 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.

Zelfs wanneer in de algemene verordening gegevensbescherming niet specifiek de aanstelling van een functionaris voor gegevensbescherming wordt vereist, kunnen organisaties het mogelijk wel interessant vinden om op vrijwillige basis een functionaris voor gegevensbescherming aan te wijzen. De Groep gegevensbescherming artikel 29 ("WP29") moedigt deze vrijwillige inspanningen aan.

Het concept van de functionaris voor gegevensbescherming is niet nieuw. Hoewel Richtlijn 95/46/EG[3] geen enkele organisatie verplicht om een functionaris voor gegevensbescherming aan te stellen, is het de voorbije jaren in verschillende lidstaten toch de gewoonte geworden om een functionaris voor gegevensbescherming aan te stellen.

Vóór de invoering van de algemene verordening gegevensbescherming argumenteerde de WP29 dat de functionaris voor gegevensbescherming de hoeksteen is van de verantwoording en dat het aanstellen van een functionaris voor gegevensbescherming de naleving kan vereenvoudigen en verder een concurrentievoordeel voor bedrijven kan vormen[4]. Naast het feit dat ze de naleving vereenvoudigen door de implementatie van verantwoordingsinstrumenten (zoals het mogelijk maken

[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), (PB L 119 van 4.5.2016). De algemene verordening gegevensbescherming is relevant voor de EER en zal van toepassing zijn nadat ze in de EER-Overeenkomst is opgenomen.

[2] Ook voor bevoegde autoriteiten is de aanstelling van een functionaris voor gegevensbescherming verplicht uit hoofde van 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 (PB L 119 van 4.5.2016, blz. 89-131), en nationale uitvoeringswetgeving. Deze richtlijnen concentreren zich weliswaar op functionarissen voor gegevensbescherming krachtens de algemene verordening gegevensbescherming, maar de vergelijkbare bepalingen in dit advies zijn ook relevant voor functionarissen voor gegevensbescherming conform 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 (PB L 281 van 23.11.1995, blz. 31).

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

van gegevensbeschermingseffectbeoordelingen en het uitvoeren of mogelijk maken van controles), fungeren functionarissen voor gegevensbescherming als tussenpersonen tussen relevante belanghebbenden (zoals toezichthoudende autoriteiten, betrokkenen en bedrijfseenheden binnen een organisatie).

Functionarissen voor gegevensbescherming zijn niet persoonlijk verantwoordelijk bij niet-naleving van de algemene verordening gegevensbescherming. In de algemene verordening gegevensbescherming staat duidelijk dat het de verwerkingsverantwoordelijke of de verwerker is die moet verzekeren en kunnen aantonen dat de verwerking in overeenstemming met de respectieve bepalingen van de algemene verordening gegevensbescherming (artikel 24, lid 1) is uitgevoerd. Naleving van de gegevensbescherming behoort tot de verantwoordelijkheid van de verwerkingsverantwoordelijke of de verwerker.

De verwerkingsverantwoordelijke of de verwerker speelt verder ook een cruciale rol in het mogelijk maken van de effectieve uitoefening van de taken van de functionaris voor gegevensbescherming. Een functionaris voor gegevensbescherming aanstellen is een eerste stap, maar functionarissen voor gegevensbescherming moeten ook voldoende autonomie en middelen krijgen om hun taken doeltreffend te kunnen uitoefenen.

In de algemene verordening gegevensbescherming wordt erkend dat de functionaris voor gegevensbescherming een sleutelfiguur is in het nieuwe systeem voor gegevensbeheer en worden regels voor zijn/haar aanwijzing, positie en taken vastgelegd. Deze richtlijnen zijn bedoeld ter verduidelijking van de relevante voorwaarden van de algemene verordening gegevensbescherming om verwerkingsverantwoordelijken en verwerkers te helpen aan de wet te voldoen, maar ook om functionarissen voor gegevensbescherming in hun functie te helpen. De richtlijnen bevatten tevens aanbevelingen voor goede praktijken op basis van in bepaalde EU-lidstaten opgedane ervaring. De WP29 houdt toezicht op de implementatie van deze richtlijnen en kan ze waar nodig met verdere details aanvullen.

2 Aanwijzing van een functionaris voor gegevensbescherming

2.1. Verplichte aanwijzing

Krachtens artikel 37, lid 1, van de algemene verordening gegevensbescherming is de aanwijzing van een functionaris voor gegevensbescherming in drie specifieke gevallen verplicht[5]:

a) wanneer de verwerking door een overheidsinstantie of overheidsorgaan wordt verricht[6];
b) wanneer de kerntaken van de verwerkingsverantwoordelijke of de verwerker bestaan uit verwerkingen die regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen; of
c) wanneer de kerntaken van de verwerkingsverantwoordelijke of de verwerker bestaan uit verwerking op grote schaal van speciale categorieën van gegevens[7] of[8] van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten[9].

[5] Merk op dat krachtens artikel 37, lid 4, de wetgeving van de Europese Unie of die van een lidstaat ook in andere situaties de aanwijzing van functionarissen voor gegevensbescherming kan eisen.

[6] Met uitzondering van rechtbanken die in hun specifieke hoedanigheid handelen. Zie artikel 32 van Richtlijn (EU) 2016/680.

In de volgende paragrafen verstrekt de WP29 advies over de criteria en de gebruikte terminologie in artikel 37, lid 1.

Tenzij duidelijk is dat een organisatie niet verplicht is om een functionaris voor gegevensbescherming aan te wijzen, raadt de WP29 verwerkingsverantwoordelijken en verwerkers aan de interne analyse te documenteren die werd uitgevoerd om te bepalen of er al of niet een functionaris voor gegevensbescherming moet worden aangesteld, teneinde aan te kunnen tonen dat met de relevante factoren correct rekening is gehouden[10]. Deze analyse maakt deel uit van de documentatie conform het verantwoordingsbeginsel. Ze kan door de toezichthoudende autoriteit worden vereist en moet wanneer nodig worden bijgewerkt, bijvoorbeeld als de verwerkingsverantwoordelijken en verwerkers nieuwe activiteiten uitvoeren of nieuwe diensten aanbieden die onder de in artikel 37, lid 1, vermelde gevallen kunnen vallen.

Wanneer een organisatie vrijwillig een functionaris voor gegevensbescherming aanwijst, gelden voor zijn of haar aanwijzing, positie en taken dezelfde voorwaarden van de artikelen 37 tot 39 die zouden gelden als de aanwijzing verplicht was geweest.

Niets verhindert een organisatie die niet wettelijk verplicht is om een functionaris voor gegevensbescherming aan te wijzen en niet vrijwillig een functionaris voor gegevensbescherming wil aanwijzen, om toch werknemers of externe adviseurs voor taken op het gebied van de bescherming van persoonsgegevens in dienst te nemen. In dit geval is het belangrijk te verzekeren dat er geen verwarring bestaat over hun functie, status, positie en taken. Daarom moet in alle communicatie binnen het bedrijf alsook met instanties voor gegevensbescherming, met betrokkenen en met het grote publiek duidelijk worden gemaakt dat deze persoon of adviseur geen functionaris voor gegevensbescherming is. [11]

De functionaris voor gegevensbescherming is, hetzij verplicht, hetzij vrijwillig, aangewezen voor alle verwerkingsactiviteiten die door de verwerkingsverantwoordelijke of de verwerker worden uitgevoerd.

2.1.1 "OVERHEIDSINSTANTIE OF OVERHEIDSORGAAN"

In de algemene verordening gegevensbescherming wordt niet gedefinieerd wat een "*overheidsinstantie of overheidsorgaan"* precies inhoudt. De WP29 is van mening dat een dergelijk begrip in de nationale wetgeving bepaald dient te worden. Bijgevolg vallen onder de term "overheidsinstanties en overheidsorganen" nationale, regionale en lokale instanties, maar uit hoofde van de geldende nationale

---

[7] Uit hoofde van artikel 9 zijn dit onder andere persoonsgegevens waaruit iemands raciale of etnische achtergrond, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of een lidmaatschap van een vakbond blijken, en de verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, gegevens over gezondheid of gegevens over het seksleven of de seksuele geaardheid van een natuurlijke persoon.

[8] In artikel 37, lid 1, onder c), wordt het woord "*en*" gebruikt. Zie punt 2.1.5 verder in dit document voor uitleg over het gebruik van "*of*" in plaats van "*en*".

[9] Artikel 10.

[10] Zie artikel 24, lid 1.

[11] Dit is ook relevant voor Chief Privacy Officers (CPO's) of andere privacy-professionals die sommige bedrijven momenteel al in dienst hebben en die mogelijk niet altijd aan de criteria van de algemene verordening gegevensbescherming beantwoorden, bijvoorbeeld wat betreft de beschikbare middelen of de waarborgen met betrekking tot onafhankelijkheid; in dat geval kunnen ze niet als functionarissen voor gegevensbescherming beschouwd en zo genoemd worden.

wetgeving omvat het concept doorgaans ook een reeks andere publiekrechtelijke instellingen[12]. In die gevallen is een aanwijzing van een functionaris voor gegevensbescherming verplicht.

Een overheidstaak mag worden uitgevoerd en publiek gezag mag worden uitgeoefend[13] door zowel overheidsinstanties of -organen als andere publiek- of privaatrechtelijke natuurlijke personen of rechtspersonen, in diverse sectoren zoals, conform de nationale regelgeving van een lidstaat, het openbaar vervoer, de water- en energievoorziening, wegeninfrastructuur, de publieke omroep, sociale huisvesting of disciplinaire instanties voor beschermde beroepen.

In deze gevallen kunnen betrokkenen zich in vrijwel dezelfde situatie bevinden als diegenen waarvan de gegevens door een overheidsinstantie of -orgaan verwerkt worden. Zo kunnen gegevens met name voor soortgelijke doelen worden verwerkt, en hebben mensen op gelijkaardige manier weinig of geen keuze of en hoe hun gegevens worden verwerkt, waardoor ze bijgevolg de aanvullende bescherming nodig hebben die met de aanwijzing van een functionaris voor gegevensbescherming kan worden bereikt.

Hoewel dat in dergelijke gevallen niet verplicht is, raadt de WP29 als een goede praktijk aan dat privaatrechtelijke organisaties die overheidstaken verrichten of publiek gezag uitoefenen, een functionaris voor gegevensbescherming aanwijzen. Zo'n functionaris voor gegevensbescherming staat in voor alle uitgevoerde verwerkingsactiviteiten, ook handelingen die niets te maken hebben met de uitvoering van een overheidstaak of de uitoefening van een officiële verplichting (bv. het beheer van een databank van medewerkers).

2.1.2 "KERNTAKEN"

In artikel 37, lid 1, onder b) en c), van de algemene verordening gegevensbescherming wordt verwezen naar de "*[verwerkingen waarmee] de verwerkingsverantwoordelijke of verwerker hoofdzakelijk is belast"*. In overweging 97 wordt gespecificeerd dat de kerntaken van een verwerkingsverantwoordelijke betrekking hebben op "*hoofdactiviteiten en niet op de verwerking van persoonsgegevens als nevenactiviteit*". "Kerntaken" kunnen worden beschouwd als de belangrijkste handelingen die nodig zijn om de doelstellingen van de verwerkingsverantwoordelijke of de verwerker te bereiken.

Dit betekent echter niet dat activiteiten waarbij de verwerking van gegevens onlosmakelijk deel uitmaakt van de activiteit van de verwerkingsverantwoordelijke of de verwerker, niet als "kerntaken" moeten worden geïnterpreteerd. Zo is het de kerntaak van een ziekenhuis gezondheidszorg te bieden. Maar een ziekenhuis kan geen veilige en efficiënte gezondheidszorg bieden zonder de verwerking van medische gegevens, zoals de medische dossiers van de patiënten. Bijgevolg moet de verwerking van dit soort gegevens als een van de kerntaken van elk ziekenhuis worden beschouwd, en moeten ziekenhuizen dus functionarissen voor gegevensbescherming aanwijzen.

Een ander voorbeeld is een privaat beveiligingsbedrijf dat instaat voor de bewaking van een aantal private winkelcentra en openbare ruimten. Bewaking is de kerntaak van het bedrijf, wat dan weer

[12] Zie bv. de definitie van "*openbaar lichaam*" en "*publiekrechtelijke instelling*" in artikel 2, leden 1 en 2, van Richtlijn 2003/98/EG van het Europees Parlement en de Raad van 17 november 2003 inzake het hergebruik van overheidsinformatie (PB L 345 van 31.12.2003, blz. 90).
[13] Artikel 6, lid 1, onder e).

onlosmakelijk verbonden is met de verwerking van persoonsgegevens. Bijgevolg moet ook dit bedrijf een functionaris voor gegevensbescherming aanwijzen.

Anderzijds voeren alle organisaties bepaalde activiteiten uit, zoals de uitbetaling van hun werknemers of standaard IT-ondersteuning. Dit zijn voorbeelden van noodzakelijke ondersteuningsfuncties voor de kerntaak of de hoofdactiviteit van de organisatie. Ook al zijn deze activiteiten noodzakelijk of essentieel, ze worden doorgaans eerder als nevenfuncties dan als kerntaak beschouwd.

2.1.3 "OP GROTE SCHAAL"

In artikel 37, lid 1, onder b) en c), is vastgelegd dat de verwerking van persoonsgegevens op grote schaal moet worden uitgevoerd om de aanwijzing van een functionaris voor gegevensbescherming nodig te maken. In de algemene verordening gegevensbescherming wordt niet gedefinieerd wat wordt bedoeld met verwerking op grote schaal. In overweging 91 wordt daarover wel enige toelichting gegeven[14].

Het is inderdaad niet mogelijk om over de hoeveelheid verwerkte gegevens of over het aantal betrokkenen precieze cijfers te geven, die in alle situaties van toepassing kunnen zijn. Dat sluit echter niet uit dat een standaardpraktijk na verloop van tijd verder uitgewerkt kan worden voor de identificatie van meer specifieke en/of kwantitatieve criteria voor wat de term "*op grote schaal*" met betrekking tot bepaalde courante verwerkingsactiviteiten inhoudt. De WP29 is ook van plan om aan deze ontwikkeling bij te dragen door voorbeelden van de relevante drempelwaarden voor de aanwijzing van een functionaris voor gegevensbescherming te delen en publiek te maken.

De WP29 raadt in ieder geval aan om met name de volgende factoren in aanmerking te nemen bij het bepalen of de verwerking al dan niet op grote schaal wordt uitgevoerd:

- Het aantal betrokkenen waarover het gaat - hetzij als een specifiek aantal of als een evenredig deel van de relevante populatie
- De hoeveelheid gegevens en/of het bereik van de verschillende verwerkte gegevensitems
- De duur of permanentie van de gegevensverwerking
- De geografische omvang van de verwerkingsactiviteit

[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 [...] een hoog risico met zich kunnen brengen*". Anderzijds wordt in de overweging specifiek bepaald 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"*. Het is belangrijk dat in gedachten wordt gehouden dat in de overweging voorbeelden worden gegeven van de uitersten op de schaal (verwerking door een individuele arts versus verwerking van gegevens van een heel land of op Europees niveau); tussen deze uitersten bevindt er zich een grote grijze zone. Verder moet ook rekening worden gehouden met het feit dat in deze overweging naar gegevensbeschermingseffectbeoordelingen wordt verwezen. Dat impliceert dat bepaalde elementen wellicht specifiek voor die context gelden en niet noodzakelijkerwijs op precies dezelfde manier op de aanduiding van functionarissen voor gegevensbescherming van toepassing zijn.

Hierna enkele voorbeelden van grootschalige verwerking:

- Verwerking van patiëntgegevens in het kader van de regelmatige bedrijfsvoering van een ziekenhuis
- Verwerking van reisgegevens van personen die van het openbaar vervoerssysteem in een stad gebruikmaken (bv. tracering via reiskaarten)
- Verwerking van realtime geolocatiegegevens van klanten van een internationale fastfoodketen voor statistische doeleinden door een verwerker die gespecialiseerd is in het leveren van dergelijke diensten
- Verwerking van klantgegevens in het kader van de regelmatige bedrijfsvoering van een verzekeringsmaatschappij of een bank
- Verwerking van persoonsgegevens met het oog op gedragsgerelateerde publiciteit door een zoekmachine
- Verwerking van gegevens (content, surfgedrag, locatie) via aanbieders van telefonie- of internetdiensten

Hierna enkele voorbeelden van verwerkingen die niet als grootschalig worden beschouwd:

- Verwerking van patiëntgegevens door een individuele arts
- Verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten door een individuele advocaat

2.1.4 "REGELMATIGE EN STELSELMATIGE OBSERVATIE"

De term "regelmatige en stelselmatige observatie" van betrokkenen wordt niet gedefinieerd in de algemene verordening gegevensbescherming, maar het concept "*controle van het gedrag van betrokkenen*" wordt in overweging 24 vermeld[15] en omvat duidelijk alle vormen van opsporing en profilering op het internet, ook met het oog op gedragsgerelateerde publiciteit.

Het begrip observatie beperkt zich echter niet tot het internet, en het online volgen van personen moet slechts worden beschouwd als één voorbeeld van observatie van het gedrag van betrokkenen[16].

De WP29 interpreteert de term "regelmatig" op een of meer van de volgende manieren:

- Iets wat doorlopend of op specifieke ogenblikken gedurende een bepaalde periode voorkomt
- Terugkerend of repetitief op vaste tijdstippen
- Iets wat zich constant of periodiek voordoet

De WP29 interpreteert de term "stelselmatig" op een of meer van de volgende manieren:

---

[15] *"Om uit te maken of een verwerking kan worden beschouwd als controle 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 ten aanzien van hem te nemen of om zijn persoonlijke voorkeuren, gedragingen en attitudes te analyseren of te voorspellen."*

[16] Merk op dat overweging 24 is gericht op de extraterritoriale toepassing van de algemene verordening gegevensbescherming. Daarenboven bestaat er altijd een verschil tussen de formuleringen "*het monitoren van hun gedrag"* (artikel 3, lid 2, onder b)) en *"regelmatige en stelselmatige observatie [...] van betrokkenen"* (artikel 37, lid 1, onder b)), waardoor ze als twee verschillende begrippen kunnen worden beschouwd.

- Iets wat zich volgens een systeem voordoet
- Vooraf geregeld, georganiseerd of methodisch
- Iets wat zich voordoet in het kader van een algemeen programma voor gegevensverzameling
- Iets wat uitgevoerd wordt in het kader van een strategie

Hierna enkele voorbeelden van activiteiten die als een regelmatige en stelselmatige observatie van betrokkenen worden beschouwd: een telecommunicatienetwerk beheren; telecommunicatiediensten leveren; retargeting via e-mail; marketingactiviteiten op basis van gegevens; profilering en scores toekennen met het oog op risicobeoordeling (bv. voor toekenning van een kredietwaardigheidsscore, bepaling van verzekeringspremies, fraudepreventie, detectie van witwaspraktijken); locatietracering, bv. via mobiele apps; programma's voor klantenbinding; gedragsgerelateerde publiciteit; monitoring van gezondheids- en conditiegegevens via draagbare apparaten; gesloten tv-circuit; gekoppelde apparaten bv. slimme meters, slimme wagens, domotica enz.

2.1.5 SPECIALE GEGEVENSCATEGORIEËN EN GEGEVENS BETREFFENDE STRAFRECHTELIJKE VEROORDELINGEN EN STRAFBARE FEITEN

Artikel 37, lid 1, onder c), betreft de verwerking van speciale gegevenscategorieën als bedoeld in artikel 9 en van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10. Hoewel in de bepaling het woord "en" wordt gebruikt, is er geen beleidsregel die stelt dat de twee criteria tegelijkertijd moeten worden toegepast. De tekst moet dan ook gelezen worden alsof er "of" stond.

2.2. Functionaris voor gegevensbescherming van de verwerker

Artikel 37 geldt voor de aanwijzing van een functionaris voor gegevensbescherming voor zowel verwerkingsverantwoordelijken[17] als verwerkers[18]. Afhankelijk van wie aan de criteria voor verplichte aanwijzing voldoet, is het in sommige gevallen alleen de verwerkingsverantwoordelijke of alleen de verwerker die een functionaris voor gegevensbescherming moet aanwijzen, terwijl dat in andere gevallen voor allebei geldt (waarbij de respectieve functionarissen dan moeten samenwerken).

Het is belangrijk te benadrukken dat zelfs als de verwerkingsverantwoordelijke aan de criteria voor verplichte aanwijzing voldoet, diens verwerker niet per definitie verplicht is een functionaris voor gegevensbescherming aan te stellen. Maar dat kan wel een goede praktijk zijn.

Voorbeelden:

- Een klein familiebedrijf dat zich bezighoudt met de distributie van huishoudtoestellen binnen één stad maakt gebruik van de diensten van een verwerker die als kerntaak websitegegevens analyseert en hulp biedt bij op internetgedrag gebaseerde publiciteit en marketing. Gezien het kleine aantal klanten en het relatief beperkte aantal activiteiten zorgen de activiteiten van het familiebedrijf en de klanten ervan niet voor een verwerking van gegevens op "grote schaal".

[17] De verwerkingsverantwoordelijke wordt in artikel 4, lid 7, gedefinieerd als de persoon of de instantie die de doelstellingen van en de middelen voor de verwerking vastlegt.

[18] De verwerker wordt in artikel 4, lid 8, gedefinieerd als de persoon of de instantie die gegevens in naam van de verwerkingsverantwoordelijke verwerkt.

De activiteiten van de verwerker, die veel klanten zoals deze kleine onderneming heeft, zijn echter wel verwerking op grote schaal. De verwerker moet daarom krachtens artikel 37, lid 1, onder b), een functionaris voor gegevensbescherming aanwijzen. Tegelijkertijd is het familiebedrijf zelf niet verplicht een functionaris voor gegevensbescherming aan te wijzen.

- Een middelgrote tegelfabrikant besteedt zijn diensten voor arbeidsgerelateerde gezondheidszorg uit aan een externe verwerker, die een groot aantal soortgelijke klanten heeft. De verwerker moet conform artikel 37, lid 1, onder c), een functionaris voor gegevensbescherming aanwijzen, aangezien de verwerking op grote schaal plaatsvindt. De fabrikant daarentegen is niet per definitie verplicht een functionaris voor gegevensbescherming aan te wijzen.

De door een verwerker aangewezen functionaris voor gegevensbescherming ziet ook toe op activiteiten die door de organisatie van de verwerkers worden uitgevoerd wanneer hij als een zelfstandige verwerkingsverantwoordelijke handelt (bv. HR, IT, logistiek).

2.3. Aanwijzing van één enkele functionaris voor gegevensbescherming voor meerdere organisaties

In artikel 37, lid 2, wordt toegestaan dat een concern één enkele functionaris voor gegevensbescherming aanstelt, op voorwaarde dat deze persoon "*vanuit elke vestiging makkelijk te contacteren is*". De notie van bereikbaarheid verwijst naar de taken van de functionaris voor gegevensbescherming als contactpersoon voor de betrokkenen[19], de toezichthoudende autoriteit[20], maar ook binnen de organisatie. Daarbij wordt ervan uitgegaan dat één van de taken van de functionaris voor gegevensbescherming erin bestaat *"de verwerkingsverantwoordelijke of de verwerker en de werknemers die verwerken, [te] informeren en adviseren over hun verplichtingen uit hoofde van deze verordening"*[21].

Om te verzekeren dat de functionaris voor gegevensbescherming, hetzij intern, hetzij extern, bereikbaar is, moet vooral verzekerd worden dat zijn contactgegevens in overeenstemming met de vereisten van de algemene verordening gegevensbescherming beschikbaar zijn[22].

Hij of zij moet, indien nodig bijgestaan door een team, in staat zijn om efficiënt met de betrokkenen te communiceren[23] en met de betreffende toezichthoudende autoriteiten samen te werken[24]. Dat

[19] Artikel 38, lid 4: "*Betrokkenen kunnen met de functionaris voor gegevensbescherming contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten uit hoofde van deze verordening*".

[20] Artikel 39, lid 1, onder e): "*optreden als contactpunt voor de toezichthoudende autoriteit 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, lid 1, onder a).

[22] Zie ook punt 2.6 hieronder.

[23] Artikel 12, lid 1: *"De verwerkingsverantwoordelijke 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, lid 1, onder d)*: "met de toezichthoudende autoriteit samenwerken"*

impliceert ook dat alle communicaties moeten plaatsvinden in de taal of talen van de betreffende toezichthoudende autoriteiten en betrokkenen. De beschikbaarheid van een functionaris voor gegevensbescherming (fysiek op dezelfde locatie als de werknemers, via een hotline of via een ander beveiligd communicatiekanaal) is van essentieel belang om te verzekeren dat de betrokkenen met de functionaris voor gegevensbescherming contact kunnen opnemen.

Krachtens artikel 37, lid 3, kan één functionaris voor gegevensbescherming worden aangewezen voor verschillende overheidsinstanties of overheidsorganen, met inachtneming van hun organisatiestructuur en omvang. Daarbij gelden dezelfde overwegingen inzake middelen en communicatie. Aangezien de functionaris voor gegevensbescherming meerdere taken heeft, moet de verwerkingsverantwoordelijke of de verwerker verzekeren dat één enkele functionaris voor gegevensbescherming, indien nodig bijgestaan door een team, deze taken efficiënt kan uitvoeren ondanks het feit dat hij voor meerdere overheidsinstanties en -organen is aangesteld.

2.4. Bereikbaarheid en lokalisatie van de functionaris voor gegevensbescherming

Volgens Afdeling 4 van de algemene verordening gegevensbescherming moet de functionaris voor gegevensbescherming makkelijk bereikbaar zijn.

Om dit te verzekeren, raadt de WP29 aan dat de functionaris voor gegevensbescherming zich binnen de Europese Unie bevindt, ongeacht het feit of de verwerkingsverantwoordelijke of de verwerker al dan niet in de Europese Unie is gevestigd.

Toch kan niet uitgesloten worden dat in sommige gevallen waarbij de verwerkingsverantwoordelijke of de verwerker geen vestiging in de Europese Unie heeft[25], een functionaris voor gegevensbescherming zijn/haar activiteiten efficiënter kan uitvoeren wanneer hij/zij buiten de EU is gevestigd.

2.5. Deskundigheid en vaardigheden van de functionaris voor gegevensbescherming

In artikel 37, lid 5, wordt bepaald dat de functionaris voor gegevensbescherming "*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*". In overweging 97 wordt bepaald dat het vereiste niveau van deskundigheid dient te worden bepaald op grond van de uitgevoerde gegevensverwerkingsactiviteiten en de bescherming die voor de verwerkte persoonsgegevens is vereist.

- **Niveau van deskundigheid**

Het vereiste niveau van deskundigheid is niet strikt gedefinieerd, maar moet in verhouding zijn tot de gevoeligheid en de complexiteit van de gegevens, alsook de hoeveelheid gegevens die een organisatie verwerkt. Bijvoorbeeld: bij een bijzonder complexe dataverwerkingsactiviteit of bij verwerking van een groot aantal gevoelige gegevens kan van de functionaris voor gegevensbescherming een hoger

[25] Zie artikel 3 van de algemene verordening gegevensbescherming over territoriaal toepassingsgebied.

niveau van deskundigheid en ondersteuning worden vereist. Verder is er ook een verschil vast te stellen naargelang de organisatie stelselmatig persoonsgegevens buiten de Europese Unie brengt, dan wel of dergelijke overdrachten slechts occasioneel zijn. De functionaris voor gegevensbescherming moet dan ook met zorg worden gekozen, met inachtneming van de problemen inzake gegevensbescherming die zich binnen de organisatie kunnen stellen.

- **Professionele kwaliteiten**

Hoewel in artikel 37, lid 5, geen professionele kwaliteiten worden gespecificeerd waarmee bij de aanwijzing van een functionaris voor gegevensbescherming rekening moet worden gehouden, is het feit dat functionarissen voor gegevensbescherming enige ervaring moeten hebben met nationale en Europese wetten en praktijken op het gebied van gegevensbescherming, alsook een grondige kennis van de algemene verordening gegevensbescherming, een relevant element. Verder is het ook interessant als de toezichthoudende autoriteiten een gepaste en regelmatige opleiding voor functionarissen voor gegevensbescherming stimuleren.

Kennis van de bedrijfstak en van de organisatie van de verwerkingsverantwoordelijke is nuttig. De functionaris voor gegevensbescherming moet ook voldoende inzicht hebben in de uitgevoerde verwerkingsactiviteiten, de informatiesystemen en de behoeften van de verwerkingsverantwoordelijke op het vlak van gegevensbeveiliging en gegevensbescherming.

Wanneer het om een overheidsinstantie of overheidsorgaan gaat, moet de functionaris voor gegevensbescherming ook een gedegen kennis hebben van de administratieve regels en procedures van de organisatie.

- **Vermogen om zijn taken te vervullen**

Het vermogen om de taken te vervullen die bij de positie van functionaris voor gegevensbescherming horen, moet worden opgevat als een verwijzing naar zijn persoonlijke vaardigheden en kennis, maar heeft ook te maken met zijn positie binnen de organisatie. Belangrijke persoonlijke kwaliteiten zijn bijvoorbeeld integriteit en een hoge mate van professionele ethiek; de belangrijkste taak van de functionaris voor gegevensbescherming is ervoor te zorgen dat de algemene verordening gegevensbescherming nageleefd wordt. De functionaris voor gegevensbescherming speelt een fundamentele rol in het creëren van een cultuur van gegevensbescherming binnen de organisatie en helpt ook bij de implementatie van essentiële elementen uit de algemene verordening gegevensbescherming, zoals de beginselen van gegevensverwerking[26], de rechten van de betrokkenen[27], gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen[28], register van verwerkingsactiviteiten[29], beveiliging van de verwerking[30] en melding van en communicatie over inbreuken met betrekking tot gegevens[31].

- **Functionaris voor gegevensbescherming op basis van een dienstverleningsovereenkomst**

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

De functie van de functionaris voor gegevensbescherming kan ook worden bekleed op basis van een dienstverleningsovereenkomst die werd afgesloten met een persoon of een organisatie die niet tot de organisatie van de verwerkingsverantwoordelijke/verwerker behoort. In dit laatste geval is het van essentieel belang dat alle leden van de organisatie die de functies van een functionaris voor gegevensbescherming bekleden, aan alle geldende vereisten vermeld in Afdeling 4 van de algemene verordening gegevensbescherming voldoen (zo is het bijvoorbeeld van essentieel belang dat er geen belangenconflicten zijn). Verder is het ook belangrijk dat al deze leden beschermd zijn uit hoofde van de bepalingen van de algemene verordening gegevensbescherming (bv. geen oneerlijke beëindiging van de dienstverleningsovereenkomst voor activiteiten als functionaris voor gegevensbescherming, maar ook geen oneerlijk ontslag van elke medewerker in de organisatie die de taken van functionaris voor gegevensbescherming uitvoert). Tegelijkertijd kunnen de individuele vaardigheden en troeven zo worden gecombineerd dat meerdere personen die als een team werken, hun klanten nog efficiënter van dienst zijn.

Met het oog op juridische transparantie en goede organisatie en om belangenconflicten bij de leden van het team te vermijden, raden we aan om de taken binnen het team van de functionaris voor gegevensbescherming duidelijk vast te leggen, alsook voor iedere klant één enkele persoon als hoofdcontactpersoon en "verantwoordelijke" aan te stellen. Algemeen genomen, zou het ook interessant zijn om deze punten in de dienstverleningsovereenkomst te specificeren.

2.6. Publicatie en communicatie van de contactgegevens van de functionaris voor gegevensbescherming

Krachtens artikel 37, lid 7, van de algemene verordening gegevensbescherming moet de verwerkingsverantwoordelijke of de verwerker:

- de contactgegevens van de functionaris voor gegevensbescherming bekendmaken, en
- de contactgegevens van de functionaris voor gegevensbescherming aan de relevante toezichthoudende autoriteiten communiceren.

Deze vereisten hebben tot doel te verzekeren dat zowel betrokkenen (zowel binnen als buiten de organisatie) als toezichthoudende autoriteiten gemakkelijk en direct met de functionaris voor gegevensbescherming contact kunnen opnemen, zonder daarbij een ander deel van de organisatie te moeten contacteren. Vertrouwelijkheid is even belangrijk: zo kunnen werknemers afkerig zijn om bij de functionaris voor gegevensbescherming een klacht in te dienen als de vertrouwelijkheid van hun mededelingen niet gegarandeerd is.
De functionaris voor gegevensbescherming is met betrekking tot de uitvoering van zijn/haar taken overeenkomstig het Unierecht of het lidstatelijk recht tot geheimhouding of vertrouwelijkheid gehouden (artikel 38, lid 5).

De contactgegevens van de functionaris voor gegevensbescherming moeten informatie omvatten die de betrokkenen en toezichthoudende instanties in staat stelt om hem/haar op een gemakkelijke manier te bereiken (een postadres, een rechtstreeks telefoonnummer en/of een specifiek e-mailadres). Wanneer van toepassing, kunnen met het oog op communicatie met het grote publiek ook andere vormen van communicatie worden voorzien, bijvoorbeeld een specifieke hotline of een speciaal contactformulier op de website van de organisatie dat rechtstreeks naar de functionaris voor gegevensbescherming wordt gestuurd.

In artikel 37, lid 7, wordt niet verplicht dat de bekendgemaakte contactgegevens ook de naam van de functionaris voor gegevensbescherming moeten vermelden. Hoewel het misschien een goede praktijk kan zijn om dat te doen, is het aan de verwerkingsverantwoordelijke of de verwerker, alsook de functionaris voor gegevensbescherming om te beslissen of dat in de specifieke omstandigheden al dan niet noodzakelijk of nuttig is[32].

Communicatie van de naam van de functionaris voor gegevensbescherming aan de toezichthoudende autoriteit is echter van essentieel belang als de functionaris voor gegevensbescherming als contactpunt tussen de organisatie en de toezichthoudende autoriteit wil optreden (artikel 39, lid 1, onder e)).

De WP29 raadt als goede praktijk ook aan dat een organisatie de naam en contactgegevens van de functionaris voor gegevensbescherming aan haar werknemers bekendmaakt. Zo zouden de naam en contactgegevens van de functionaris voor gegevensbescherming intern op het intranet van de organisatie, in de bedrijfstelefoongids en in organogrammen kunnen worden gepubliceerd.

3 Positie van de functionaris voor gegevensbescherming

3.1. Betrokkenheid van de functionaris voor gegevensbescherming bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens

In artikel 38 van de algemene verordening gegevensbescherming wordt bepaald dat de verwerkingsverantwoordelijke en de verwerker ervoor moeten zorgen dat de functionaris voor gegevensbescherming *"naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens"*.

Het is van cruciaal belang dat de functionaris voor gegevensbescherming, of diens team, zo vroeg mogelijk betrokken wordt bij alle aangelegenheden die met gegevensbescherming verband houden. Wat betreft gegevensbeschermingseffectbeoordelingen, wordt in de algemene verordening gegevensbescherming expliciet vermeld dat de functionaris voor gegevensbescherming daarbij vroeg moet worden betrokken en gespecificeerd dat de verwerkingsverantwoordelijke bij de uitvoering van dergelijke effectbeoordelingen aan de functionaris voor gegevensbescherming advies moet vragen[33]. Door ervoor te zorgen dat de functionaris voor gegevensbescherming van bij de start geïnformeerd en geconsulteerd wordt, wordt de naleving van de algemene verordening gegevensbescherming mogelijk gemaakt en wordt een privacy-aanpak door ontwerp bevorderd, die dan ook de standaardprocedure binnen het bestuur van de organisatie moet worden. Verder is het ook belangrijk dat de functionaris voor gegevensbescherming als een gesprekspartner binnen de organisatie wordt gezien en dat hij/zij deel uitmaakt van de relevante werkgroepen die zich met gegevensverwerking binnen de organisatie bezighouden.

Bijgevolg moet de organisatie bijvoorbeeld verzekeren dat:

[32] Merk op dat in artikel 33, lid 3, onder b), waarin wordt beschreven welke informatie aan de toezichthoudende autoriteit en de betrokkenen moet worden bezorgd bij een inbreuk op persoonsgegevens, in tegenstelling tot in artikel 37, lid 7, specifiek ook wordt opgelegd dat de naam (en niet alleen de contactgegevens) van de functionaris voor gegevensbescherming moet worden gecommuniceerd.
[33] Artikel 35, lid 2.

- de functionaris voor gegevensbescherming regelmatig wordt uitgenodigd om vergaderingen van het hogere management en het middenkader bij te wonen;
- zijn/haar aanwezigheid wordt aanbevolen wanneer beslissingen worden genomen die gevolgen hebben voor de gegevensbescherming. Alle relevante informatie moet tijdig aan de functionaris voor gegevensbescherming worden bezorgd, zodat hij/zij passend advies kan verlenen;
- de mening van de functionaris voor gegevensbescherming naar behoren in overweging wordt genomen. Bij onenigheid raadt de WP29 als goede praktijk aan om de redenen voor het niet volgen van het advies van de functionaris voor gegevensbescherming te documenteren;
- de functionaris voor gegevensbescherming meteen wordt geconsulteerd zodra zich een gegevensinbreuk of een ander incident voordoet.

Waar van toepassing, kan de verwerkingsverantwoordelijke of de verwerker richtlijnen of programma's inzake gegevensbescherming uitwerken, waarin wordt vastgelegd wanneer de functionaris voor gegevensbescherming moet worden geconsulteerd.

3.2. Benodigde middelen

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

- Actieve ondersteuning van de functie van functionaris voor gegevensbescherming door het hogere management (zoals op niveau van de raad van bestuur).
- Voldoende tijd voor de functionarissen voor gegevensbescherming om hun taken te vervullen. Dit is vooral belangrijk wanneer een interne functionaris voor gegevensbescherming op deeltijdse basis is aangesteld of wanneer de externe functionaris voor gegevensbescherming naast zijn andere taken ook voor gegevensbescherming instaat. Tegenstrijdige prioriteiten zouden er anders toe kunnen leiden dat de taken van de functionaris voor gegevensbescherming verwaarloosd worden. Voldoende tijd hebben om zich aan de taken als functionaris voor gegevensbescherming te kunnen wijden is van het grootste belang. Het is een goede praktijk om een bepaald percentage van de beschikbare tijd voor de taken van functionaris voor gegevensbescherming vast te leggen, wanneer deze functie niet op voltijdse basis wordt bekleed. Verder is het ook een goede praktijk om de benodigde tijd voor de uitvoering van de functie te bepalen, alsook het gepaste prioriteitsniveau voor de taken als functionaris voor gegevensbescherming, en dient de functionaris voor gegevensbescherming (of de organisatie) een werkprogramma op te stellen.
- Adequate ondersteuning op het vlak van financiële middelen, infrastructuur (kantoren, faciliteiten, apparatuur) en personeel waar van toepassing.
- Officiële bekendmaking van de aanstelling van de functionaris voor gegevensbescherming aan alle personeelsleden om te verzekeren dat iedereen in de organisatie op de hoogte is van het bestaan van deze functie.
- Noodzakelijke toegang tot andere diensten zoals HR, juridische dienst, IT, beveiliging enz., zodat de functionarissen voor gegevensbescherming van die andere diensten de benodigde essentiële ondersteuning, bijstand of informatie kunnen ontvangen.

- Voortgezette opleiding. Functionarissen voor gegevensbescherming moeten de kans krijgen om op de hoogte te blijven van nieuwe ontwikkelingen op het vlak van gegevensbescherming. Daarbij moet het de bedoeling zijn het niveau van de deskundigheid van de functionarissen voor gegevensbescherming permanent te verhogen en hen aan te moedigen deel te nemen aan opleidingen over gegevensbescherming en aan andere vormen van professionele ontplooiing, zoals deelname aan fora over privacy, workshops enz.
- Gezien de grootte en structuur van de organisatie kan het nodig zijn om een team rond de functionaris voor gegevensbescherming samen te stellen (een functionaris voor gegevensbescherming en zijn/haar personeelsleden). In die gevallen moeten de interne structuur van het team en de taken en verantwoordelijkheden van ieder lid duidelijk worden vastgelegd. Wanneer de functie van functionaris voor gegevensbescherming door een externe dienstverlener wordt bekleed, kan op dezelfde manier een team van personen die voor die entiteit werken feitelijk alle taken van de functionaris voor gegevensbescherming als team uitvoeren, onder de verantwoordelijkheid van een aangestelde hoofdcontactpersoon van de klant.

Doorgaans moeten aan de functionaris voor gegevensbescherming meer middelen ter beschikking worden gesteld naarmate de verwerkingsactiviteiten complexer en/of gevoeliger zijn. De functie voor gegevensbescherming moet efficiënt zijn en over voldoende middelen beschikken in verhouding tot de uitgevoerde gegevensverwerking.

3.3. Instructies en "hun taken en verplichtingen onafhankelijk vervullen"

In artikel 38, lid 3, worden enkele basiswaarborgen vastgelegd om te helpen verzekeren dat functionarissen voor gegevensbescherming hun taken voldoende autonoom binnen de organisatie kunnen vervullen. Daarbij moeten vooral verwerkingsverantwoordelijken/verwerkers ervoor zorgen dat de functionaris voor gegevensbescherming "*geen instructies ontvangt met betrekking tot de uitvoering van [zijn of haar] taken"*. In overweging 97 wordt toegevoegd dat functionarissen voor gegevensbescherming "*dienen in staat te zijn hun taken en verplichtingen onafhankelijk te vervullen, ongeacht of zij in dienst zijn van de verwerkingsverantwoordelijke*".

Dit betekent dat functionarissen voor gegevensbescherming bij het vervullen van hun taken krachtens artikel 39 geen instructies mogen ontvangen over hoe ze een bepaalde aangelegenheid moeten behandelen, bijvoorbeeld tot welk resultaat ze moeten komen, hoe ze een klacht moeten onderzoeken, of nog of ze al dan niet de toezichthoudende autoriteit moeten raadplegen. Daarenboven mogen ze ook geen instructies ontvangen om een bepaald standpunt in te nemen in een aangelegenheid die verband houdt met de wet op de gegevensbescherming, bijvoorbeeld een specifieke interpretatie van de wet.

Het autonome karakter van de functionarissen voor gegevensbescherming betekent echter niet dat ze over meer beslissingsbevoegdheid beschikken dan voor hun taken krachtens artikel 39 vereist is.

De verwerkingsverantwoordelijke of verwerker blijft verantwoordelijk voor de naleving van de wetten inzake gegevensbescherming en moet die naleving ook kunnen aantonen[34]. Als de verwerkingsverantwoordelijke of de verwerker beslissingen nemen die niet in de lijn liggen van de algemene verordening gegevensbescherming en het advies van de functionaris voor

[34] Artikel 5, lid 2.

gegevensbescherming, moet deze laatste de kans krijgen om zijn/haar afwijkende mening duidelijk te maken aan de hoogste leidinggevende en aan diegenen die de beslissingen nemen. In dat opzicht wordt in artikel 38, lid 3, voorzien dat de functionaris voor gegevensbescherming "*rechtstreeks verslag [uitbrengt] aan de hoogste leidinggevende van de verwerkingsverantwoordelijke of de verwerker"*. Via een dergelijke directe rapportage wordt verzekerd dat het hogere management (bv. de raad van bestuur) op de hoogte is van het advies en de aanbevelingen die de functionaris voor gegevensbescherming verstrekt in het kader van zijn missie om de verwerkingsverantwoordelijke of de verwerker te informeren en te adviseren. Een ander voorbeeld van directe rapportage is het ontwerpen van een jaarverslag van de activiteiten van de functionaris voor gegevensbescherming voor de hoogste leidinggevenden.

3.4. Ontslag of sancties voor de uitvoering van taken als functionaris voor gegevensbescherming

In artikel 38, lid 3, wordt bepaald dat functionarissen voor gegevensbescherming *"door de verwerkingsverantwoordelijke of de verwerker niet ontslagen of gestraft [worden] voor de uitvoering van [hun] taken"*.

Deze vereiste verstevigt de autonome positie van de functionarissen voor gegevensbescherming en helpt te verzekeren dat ze onafhankelijk handelen en over voldoende bescherming beschikken om hun taken op het vlak van gegevensbescherming te vervullen.

Sancties zijn alleen verboden krachtens de algemene verordening gegevensbescherming als ze zijn opgelegd als gevolg van het feit dat de functionaris voor gegevensbescherming zijn/haar verplichtingen als functionaris voor gegevensbescherming heeft vervuld. Zo kan een functionaris voor gegevensbescherming bijvoorbeeld van mening zijn dat een bepaalde verwerking naar alle waarschijnlijkheid tot een hoog risico zal leiden en de verwerkingsverantwoordelijke of de verwerker adviseren om een gegevensbeschermingseffectbeoordeling uit te voeren, maar waarbij de verwerkingsverantwoordelijke of de verwerker echter niet instemt met het oordeel van de functionaris voor gegevensbescherming. In een dergelijke situatie kan de functionaris voor gegevensbescherming niet ontslagen worden voor het verlenen van dit advies.

Sancties kunnen diverse vormen aannemen en kunnen zowel direct als indirect zijn. Zo kunnen ze bijvoorbeeld bestaan uit het weigeren of uitstellen van promotie; het verhinderen van verdere uitbouw van de carrière; het weigeren van voordelen die andere werknemers krijgen. Het is niet noodzakelijk dat deze sancties ook effectief worden uitgevoerd, alleen al de dreiging volstaat, zolang het de bedoeling is daarmee de functionaris voor gegevensbescherming te straffen om redenen die te maken hebben met zijn/haar activiteiten als functionaris voor gegevensbescherming.

Als normale procedure binnen de bedrijfsvoering en zoals ook het geval zou zijn voor elke andere werknemer of aannemer krachtens en in toepassing van een geldende nationale overeenkomst of arbeids- en strafwetgeving, kan een functionaris voor gegevensbescherming nog steeds rechtmatig worden ontslagen om andere redenen dan voor het uitvoeren van zijn/haar taken als functionaris voor gegevensbescherming (bv. bij diefstal, fysieke, psychologische of seksuele intimidatie of gelijkaardig ernstig wangedrag).

In dit kader moeten we ook opmerken dat in de algemene verordening gegevensbescherming niet wordt gespecificeerd hoe en wanneer een functionaris voor gegevensbescherming ontslagen of door

iemand anders vervangen kan worden. Maar hoe solider het contract met de functionaris voor gegevensbescherming is en hoe meer waarborgen er tegen oneerlijk ontslag zijn, des te waarschijnlijker is het dat ze autonoom zullen kunnen handelen. Daarom verwelkomt de WP29 alle inspanningen van organisaties op dit vlak.

3.5. Belangenconflicten

Krachtens artikel 38, lid 6, kunnen functionarissen voor gegevensbescherming "*andere taken en plichten vervullen"*. Daartoe moet de organisatie er echter voor zorgen dat "*deze taken of plichten niet tot een belangenconflict leiden"*.

Het uitblijven van een belangenconflict hangt nauw samen met de vereiste om autonoom te handelen. Hoewel functionarissen voor gegevensbescherming andere functies kunnen bekleden, kunnen hen alleen andere taken en plichten worden toevertrouwd als deze geen aanleiding geven tot enig belangenconflict. Dit houdt met name in dat de functionaris voor gegevensbescherming binnen de organisatie geen functie kan bekleden waarbij hij of zij de doelstellingen van en de middelen voor de verwerking van persoonsgegevens moet bepalen. Gezien de specifieke organisatiestructuur van elke organisatie moet dit geval per geval worden beoordeeld.

Als vuistregel worden binnen de organisatie als functies met een belangenconflict beschouwd: functies in het hogere management (bv. Chief Executive, Chief Operating, Chief Financial, Chief Medical Officer, hoofd van de marketingafdeling, hoofd van Human Resources of hoofd van de IT-afdeling), maar ook lagere functies binnen de organisatiestructuur als deze personen de doelstellingen van en middelen voor de verwerking van gegevens moeten bepalen. Daarenboven kan een belangenconflict zich bijvoorbeeld ook voordoen wanneer aan een externe functionaris voor gegevensbescherming wordt gevraagd om de verwerkingsverantwoordelijke of de verwerker te vertegenwoordigen in de rechtbank bij rechtszaken over problemen met de gegevensbescherming.

Afhankelijk van de activiteiten, de grootte en de structuur van de organisatie kan het voor verwerkingsverantwoordelijken of verwerkers een goede praktijk zijn om:

- de posities te identificeren die incompatibel kunnen zijn met de functie van functionaris voor gegevensbescherming;
- interne regels daartoe op te stellen om belangenconflicten te vermijden;
- een meer algemene uitleg over belangenconflicten op te nemen;
- te verklaren dat hun functionaris voor gegevensbescherming geen belangenconflict heeft in zijn functie als functionaris voor gegevensbescherming, als een manier om anderen voor deze vereiste te sensibiliseren;
- in het huisreglement van de organisatie waarborgen op te nemen en ervoor te zorgen dat de vacature voor de positie van functionaris voor gegevensbescherming of de dienstverleningsovereenkomst voldoende gepreciseerd en gedetailleerd is om belangenconflicten te vermijden. In dit verband moeten we rekening houden met het feit dat belangenconflicten diverse vormen kunnen aannemen, afhankelijk van het feit of de functionaris voor gegevensbescherming intern of extern is gerekruteerd.

4 Taken van de functionaris voor gegevensbescherming

4.1. Controle op naleving van de algemene verordening gegevensbescherming

In artikel 39, lid 1, onder b), wordt aan functionarissen voor gegevensbescherming, naast andere taken, ook de taak opgelegd om de naleving van de algemene verordening gegevensbescherming te controleren. In overweging 97 wordt verder gespecificeerd dat de functionaris voor gegevensbescherming "*de verwerkingsverantwoordelijke of de verwerker [moet bijstaan] bij het toezicht op de interne naleving van deze verordening*".

In het kader van de taken met betrekking tot de controle op de naleving moeten functionarissen voor gegevensbescherming met name:

- informatie verzamelen om verwerkingsactiviteiten te identificeren;
- de naleving van verwerkingsactiviteiten analyseren en controleren;
- de verwerkingsverantwoordelijke of de verwerker informeren, adviseren en aanbevelingen doen.

Controle op naleving betekent niet dat de functionaris voor gegevensbescherming persoonlijk verantwoordelijk is bij een eventuele niet-naleving. In de algemene verordening gegevensbescherming staat duidelijk dat het de verwerkingsverantwoordelijke, en niet de functionaris voor gegevensbescherming is die *passende technische en organisatorische maatregelen [treft] om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd*" (artikel 24, lid 1). Naleving van gegevensbescherming behoort tot de professionele verantwoordelijkheid van de verwerkingsverantwoordelijke, niet van de functionaris voor gegevensbescherming.

4.2. Rol van de functionaris voor gegevensbescherming bij een gegevensbeschermingseffectbeoordeling

In overeenstemming met artikel 35, lid 1, is het de taak van de verwerkingsverantwoordelijke, niet van de functionaris voor gegevensbescherming, om waar nodig een gegevensbeschermingseffectbeoordeling uit te voeren. De functionaris voor gegevensbescherming kan echter wel een erg belangrijke en nuttige rol spelen door de verwerkingsverantwoordelijke te helpen. In lijn met het principe van de gegevensbescherming door ontwerp wordt in artikel 35, lid 2, specifiek opgelegd dat de verwerkingsverantwoordelijke bij de uitvoering van een gegevensbeschermingseffectbeoordeling "*advies [inwint]"* bij de functionaris voor gegevensbescherming. In artikel 39, lid 1, onder c), daarentegen, wordt aan de functionaris voor gegevensbescherming de verplichting opgelegd om "*desgevraagd advies [te] verstrekken met betrekking tot de gegevensbeschermingseffectbeoordeling en [toe te zien] op de uitvoering daarvan in overeenstemming met artikel 35*".

De WP29 raadt de verwerkingsverantwoordelijke aan advies te vragen aan de functionaris voor gegevensbescherming over onder andere de volgende aangelegenheden[35]:

[35] In artikel 39, lid 1, worden de taken van de functionaris voor gegevensbescherming vermeld en wordt aangegeven dat de functionaris voor gegevensbescherming "*ten minste"* de volgende taken vervult. Bijgevolg verhindert niets de verwerkingsverantwoordelijke om de functionaris voor gegevensbescherming andere taken

- of er al dan niet een gegevensbeschermingseffectbeoordeling moet worden uitgevoerd;
- welke methodologie bij een gegevensbeschermingseffectbeoordeling moet worden gevolgd;
- of de gegevensbeschermingseffectbeoordeling intern uitgevoerd of uitbesteed moet worden;
- welke waarborgen (waaronder technische en organisatorische maatregelen) moeten worden toegepast om eventuele risico's voor de rechten en belangen van de betrokkenen te beperken;
- of de gegevensbeschermingseffectbeoordeling al dan niet correct is uitgevoerd en of de conclusies (de verwerking al dan niet uitvoeren en welke waarborgen toepassen) al dan niet in overeenstemming zijn met de algemene verordening gegevensbescherming.

Als de verwerkingsverantwoordelijke niet met het door de functionaris voor gegevensbescherming verleende advies instemt, moet in de documentatie over de gegevensbeschermingseffectbeoordeling specifiek en schriftelijk worden gemotiveerd waarom met het advies geen rekening is gehouden[36].

De WP29 raadt de verwerkingsverantwoordelijke verder aan om bijvoorbeeld in de overeenkomst van de functionaris voor gegevensbescherming, maar ook in informatie die aan werknemers, management (en andere betrokkenen, indien van toepassing) wordt verstrekt, duidelijk de precieze taken van de functionaris voor gegevensbescherming en hun omvang vast te leggen, met name wat betreft het uitvoeren van een gegevensbeschermingseffectbeoordeling.

4.3. Samenwerken met de toezichthoudende autoriteit en handelen als contactpunt

Krachtens artikel 39, lid 1, onder d) en e), moet de functionaris voor gegevensbescherming "*met de toezichthoudende autoriteit samenwerken*" en "*optreden als contactpunt voor de toezichthoudende autoriteit 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"*.

Deze taken verwijzen naar de rol van "bemiddelaar" van de functionaris voor gegevensbescherming die in de inleiding van deze Richtlijnen werd vermeld. De functionaris voor gegevensbescherming fungeert als contactpunt om de toezichthoudende autoriteit vlotter toegang te verlenen tot alle documenten en informatie over de uitvoering van de taken vermeld in artikel 57, alsook over de uitoefening van haar onderzoeks-, corrigerende, autorisatie- en adviesbevoegdheden vermeld in artikel 58. Zoals reeds vermeld, is de functionaris voor gegevensbescherming met betrekking tot de uitvoering van zijn/haar taken overeenkomstig het Unierecht of het lidstatelijk recht tot geheimhouding of vertrouwelijkheid gehouden (artikel 38, lid 5). De verplichting tot geheimhouding/vertrouwelijkheid verhindert de functionaris voor gegevensbescherming echter niet om met de toezichthoudende autoriteit contact op te nemen en haar om advies te vragen. In artikel 39, lid 1, onder e), wordt bepaald dat de functionaris voor gegevensbescherming de toezichthoudende autoriteit voor eender welke aangelegenheid kan consulteren, wanneer dat relevant is.

---

toe te wijzen dan de taken die expliciet in artikel 39, lid 1, worden vermeld, of om die taken meer in detail te specificeren.

[36] In artikel 24, lid 1, is bepaald 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*".

4.4. Risicogebaseerde aanpak

In artikel 39, lid 2, wordt opgelegd dat de functionaris voor gegevensbescherming "*naar behoren rekening [houdt] met het aan de verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden*".

Dit artikel baseert zich op een algemeen principe waarin het gezond verstand wordt gevolgd en dat relevant kan zijn voor heel wat aspecten van de dagelijkse werkzaamheden van een functionaris voor gegevensbescherming. In feite wordt in dit artikel opgelegd dat functionarissen voor gegevensbescherming hun activiteiten moeten prioriteren en hun inspanningen moeten richten op zaken die een hoger risico voor de gegevensbescherming inhouden. Dit betekent niet dat ze de controle op de naleving van de gegevensverwerkingsactiviteiten, die in vergelijking een lager risiconiveau inhouden, moeten achterwege laten, maar het geeft wel aan dat ze zich voornamelijk moeten richten op de activiteiten met een hoger risico.

Deze selectieve en pragmatische aanpak helpt functionarissen voor gegevensbescherming om de verwerkingsverantwoordelijke te adviseren over de bij het uitvoeren van een gegevensbeschermingseffectbeoordeling te gebruiken methode, de zaken die bij een intern of extern gegevensbeschermingsonderzoek onderzocht dienen te worden, de interne opleidingen die aan de voor de verwerking verantwoordelijke medewerkers of directieleden gegeven dienen te worden en aan welke verwerkingsactiviteiten hij/zij meer tijd en middelen moet besteden.

4.5. Rol van de functionaris voor gegevensbescherming in het bijhouden van registers

Conform artikel 30, lid 1 en lid 2, is het de verwerkingsverantwoordelijke of de verwerker, en niet de functionaris voor gegevensbescherming, die "*een register [houdt] van de verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden*" of *"een register [houdt] van alle categorieën van verwerkingsactiviteiten die ten behoeve van een verwerkingsverantwoordelijke worden verricht"*.

In de praktijk zijn het vaak de functionarissen voor gegevensbescherming die inventarissen opmaken en een register van de verwerkingsactiviteiten bijhouden op basis van informatie die hen wordt verleend door de diverse afdelingen in hun organisatie die voor de verwerking van persoonsgegevens instaan. Deze praktijk werd opgesteld in overeenstemming met verschillende bestaande nationale wetten en conform de regels inzake gegevensbescherming die op de Europese instellingen en organen van toepassing zijn[37].

In artikel 39, lid 1, wordt een lijst opgesomd van de taken die de functionaris voor gegevensbescherming ten minste moet vervullen. Niets weerhoudt de verwerkingsverantwoordelijke of de verwerker er dan ook van om de functionaris voor gegevensbescherming te belasten met het bijhouden van het register van de verwerkingsactiviteiten, onder toezicht van de verwerkingsverantwoordelijke of de verwerker. Een dergelijk register moet beschouwd worden als een van de hulpmiddelen voor de functionaris voor gegevensbescherming om zijn taken uit te voeren, met name toezien op de naleving, alsook informatie verlenen aan en adviseren van de verwerkingsverantwoordelijke of de verwerker.

In ieder geval moet het register dat krachtens artikel 30 wordt bijgehouden, ook worden beschouwd als een instrument dat de verwerkingsverantwoordelijke en de toezichthoudende autoriteit in staat stelt

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

om, op aanvraag, een overzicht te krijgen van alle activiteiten van een organisatie waarbij persoonsgegevens worden verwerkt. Bijgevolg is dit dan een voorafgaande vereiste met het oog op naleving, en als dusdanig een effectieve maatregelen met het oog op verantwoording.

5 BIJLAGE - RICHTLIJNEN VOOR DE FUNCTIONARIS VOOR GEGEVENSBESCHERMING: WAT U MOET WETEN

Deze bijlage heeft tot doel in een eenvoudig en makkelijk leesbaar formaat te antwoorden op enkele essentiële vragen die organisaties zich eventueel stellen over de in de algemene verordening gegevensbescherming vastgelegde eisen voor de aanstelling van een functionaris voor gegevensbescherming.

Aanwijzing van de functionaris voor gegevensbescherming

1 Welke organisaties moeten een functionaris voor gegevensbescherming aanstellen?

De aanwijzing van een functionaris voor gegevensbescherming is verplicht:

- als de verwerking door een overheidsinstantie of overheidsorgaan wordt verricht (ongeacht het type gegevens dat wordt verwerkt);
- als de kerntaken van de verwerkingsverantwoordelijke of de verwerker bestaan uit verwerkingen die regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen;
- als de kerntaken van de verwerkingsverantwoordelijke of de verwerker bestaan uit verwerking op grote schaal van speciale categorieën van gegevens of van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten.

Merk op dat de wetgeving van de Unie of van een lidstaat ook in andere situaties de aanwijzing van DPO's kan eisen. Tot slot: zelfs als de aanwijzing van een functionaris voor gegevensbescherming niet verplicht is, kunnen organisaties het soms nuttig vinden om vrijwillig een functionaris voor gegevensbescherming aan te wijzen. De Groep gegevensbescherming artikel 29 ("WP29") moedigt deze vrijwillige inspanningen aan. Wanneer een organisatie vrijwillig een functionaris voor gegevensbescherming aanwijst, gelden voor zijn of haar aanwijzing, positie en taken dezelfde voorwaarden die zouden gelden als de aanwijzing verplicht was geweest.

Bron: Artikel 37, lid 1 van de algemene verordening gegevensbescherming

2 Wat betekent "kerntaken"?

"Kerntaken" kunnen worden beschouwd als de belangrijkste handelingen die gesteld worden met het oog op het bereiken van de doelstellingen van de verwerkingsverantwoordelijke of de verwerker. Deze omvatten ook alle activiteiten waarbij het verwerken van gegevens onlosmakelijk deel uitmaakt van de activiteit van de verwerkingsverantwoordelijke of de verwerker. Zo moet de verwerking van medische gegevens, zoals medische dossiers van patiënten, worden beschouwd als een van de kerntaken van eender welk ziekenhuis en moeten ziekenhuizen functionarissen voor gegevensbescherming aanstellen.

Anderzijds voeren alle organisaties ondersteunende activiteiten uit, bijvoorbeeld de uitbetaling van hun werknemers of standaard IT-ondersteuning. Dit zijn voorbeelden van noodzakelijke ondersteuningsfuncties voor de kerntaak of de hoofdactiviteit van de organisatie. Ook al zijn deze activiteiten noodzakelijk of essentieel, ze worden doorgaans eerder als nevenfuncties dan als kerntaak beschouwd.

Bron: Artikel 37, lid 1, onder b) en c), van de algemene verordening gegevensbescherming

3 Wat betekent "op grote schaal"?

In de algemene verordening gegevensbescherming wordt niet gedefinieerd wat precies wordt bedoeld met "op grote schaal". De WP29 raadt aan om met name de volgende factoren in aanmerking te nemen bij het bepalen of de verwerking op grote schaal wordt uitgevoerd:

- Het aantal betrokkenen waarover het gaat - hetzij als een specifiek aantal of als een evenredig deel van de relevante populatie
- De hoeveelheid gegevens en/of het bereik van de verschillende verwerkte gegevensitems
- De duur of permanentie van de gegevensverwerking
- De geografische omvang van de verwerkingsactiviteit

Hierna enkele voorbeelden van verwerking op grote schaal:

- Verwerking van patiëntgegevens in het kader van de regelmatige bedrijfsvoering van een ziekenhuis
- Verwerking van reisgegevens van personen die van het openbaar vervoerssysteem in een stad gebruikmaken (bv. tracering via reiskaarten)
- Verwerking van realtime geolocatiegegevens van klanten van een internationale fastfoodketen met het oog op statistische verwerking door een daarin gespecialiseerde dienst
- Verwerking van klantgegevens in het kader van de regelmatige bedrijfsvoering van een verzekeringsmaatschappij of een bank
- Verwerking van persoonsgegevens met het oog op gedragsgerelateerde publiciteit door een zoekmachine
- Verwerking van gegevens (content, surfgedrag, locatie) via aanbieders van telefonie- of internetdiensten

Hierna enkele voorbeelden van verwerkingen die niet als grootschalig worden beschouwd:

- Verwerking van patiëntgegevens door een individuele arts
- Verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten door een individuele advocaat

Bron: Artikel 37, lid 1, onder b) en c), van de algemene verordening gegevensbescherming

4 Wat betekent "regelmatige en stelselmatige observatie"?

De term "regelmatige en stelselmatige observatie" van betrokkenen wordt niet gedefinieerd in de algemene verordening gegevensbescherming, maar omvat duidelijk alle vormen van opsporing en profilering op het internet, ook met het oog op gedragsgerelateerde publiciteit. Het begrip "observatie" beperkt zich echter niet tot het internet.

Hierna enkele voorbeelden van activiteiten die als een regelmatige en stelselmatige observatie van betrokkenen worden beschouwd: een telecommunicatienetwerk beheren; telecommunicatiediensten leveren; retargeting via e-mail; marketingactiviteiten op basis van gegevens; profilering en scores toekennen met het oog op risicobeoordeling (bv. voor toekenning van een kredietwaardigheidsscore, bepaling van verzekeringspremies, fraudepreventie, detectie van witwaspraktijken); locatietracering, bv. via mobiele apps; programma's voor klantenbinding; gedragsgerelateerde publiciteit; monitoring van gezondheids- en conditiegegevens via draagbare apparaten; gesloten tv-circuit; gekoppelde apparaten bv. slimme meters, slimme wagens, domotica enz.

De WP29 interpreteert de term "regelmatig" op een of meer van de volgende manieren:

- Iets wat doorlopend of op specifieke ogenblikken gedurende een bepaalde periode voorkomt
- Terugkerend of repetitief op vaste tijdstippen
- Iets wat zich constant of periodiek voordoet

De WP29 interpreteert de term "stelselmatig" op een of meer van de volgende manieren:

- Iets wat zich volgens een systeem voordoet
- Vooraf geregeld, georganiseerd of methodisch
- Iets wat zich voordoet in het kader van een algemeen programma voor gegevensverzameling
- Iets wat wordt uitgevoerd in het kader van een strategie

Bron: Artikel 37, lid 1, onder b), van de algemene verordening gegevensbescherming

5 Kunnen organisaties gezamenlijk een functionaris voor gegevensbescherming aanstellen? Zo ja, onder welke voorwaarden?

Ja. Een concern kan één enkele functionaris voor gegevensbescherming aanstellen, op voorwaarde dat deze persoon "*vanuit elke vestiging makkelijk te contacteren is*". De notie van bereikbaarheid verwijst naar de taken van de functionaris voor gegevensbescherming als contactpersoon voor de betrokkenen, de toezichthoudende autoriteit alsook binnen de organisatie. Om te verzekeren dat de functionaris voor gegevensbescherming, hetzij intern, hetzij extern, bereikbaar is, moet vooral verzekerd worden dat diens contactgegevens in overeenstemming met de algemene verordening gegevensbescherming beschikbaar zijn. De functionaris voor gegevensbescherming moet, indien nodig bijgestaan door een team, in staat zijn om efficiënt met de betrokkenen te communiceren en met de betreffende toezichthoudende autoriteiten samen te werken. Met andere woorden: alle communicaties moeten plaatsvinden in de taal of talen van de betreffende toezichthoudende autoriteiten en betrokkenen. De beschikbaarheid van een functionaris voor gegevensbescherming (fysiek op dezelfde locatie als de werknemers, via een hotline of via een ander beveiligd communicatiekanaal) is van essentieel belang om te verzekeren dat de betrokkenen met de functionaris voor gegevensbescherming contact kunnen opnemen.

Een enkele functionaris voor gegevensbescherming kan voor verschillende overheidsinstanties of overheidsorganen worden aangewezen, met inachtneming van hun organisatiestructuur en omvang. Daarbij gelden dezelfde overwegingen inzake middelen en communicatie. Aangezien de functionaris voor gegevensbescherming meerdere taken heeft, moet de verwerkingsverantwoordelijke of de verwerker verzekeren dat één enkele functionaris voor gegevensbescherming, indien nodig bijgestaan door een team, deze taken efficiënt kan uitvoeren ondanks het feit dat hij voor meerdere overheidsinstanties en -organen is aangesteld.

Bron: Artikel 37, lid 2 en lid 3, van de algemene verordening gegevensbescherming

6 Waar moet de functionaris voor gegevensbescherming gevestigd zijn?

Om dit te verzekeren, raadt de WP29 aan dat de functionaris voor gegevensbescherming zich binnen de Europese Unie bevindt, ongeacht het feit of de verwerkingsverantwoordelijke of de verwerker al dan niet in de Europese Unie gevestigd is. Toch kan niet worden uitgesloten dat in sommige gevallen waarbij de verwerkingsverantwoordelijke of de verwerker geen vestiging in de Europese Unie heeft,

een functionaris voor gegevensbescherming zijn/haar activiteiten efficiënter kan uitvoeren wanneer hij/zij buiten de EU gevestigd is.

7 Kan er een externe functionaris voor gegevensbescherming worden aangesteld?

Ja. De functionaris voor gegevensbescherming kan een personeelslid van de verwerkingsverantwoordelijke of de verwerker (interne functionaris voor gegevensbescherming) zijn, of kan de taken op grond van een dienstverleningsovereenkomst verrichten. Dat betekent dat de functionaris voor gegevensbescherming ook een derde kan zijn die zijn/haar functie uitoefent op basis van een dienstverleningsovereenkomst die met een individu of een organisatie werd afgesloten.

Wanneer de functie van functionaris voor gegevensbescherming door een externe dienstverlener wordt bekleed, kan een team van personen die voor die entiteit werken feitelijk alle taken van de functionaris voor gegevensbescherming als team uitvoeren, onder de verantwoordelijkheid van een voor de klant aangestelde hoofdcontactpersoon en "verantwoordelijke". In dit geval is het van essentieel belang dat alle leden van de externe organisatie die de taken van de functionaris voor gegevensbescherming op zich nemen, aan alle geldende eisen van de algemene verordening gegevensbescherming voldoen.

Met het oog op juridische transparantie en goede organisatie en om belangenconflicten bij de leden van het team te vermijden, wordt in de Richtlijnen aangeraden om de taken binnen het team van de externe functionaris voor gegevensbescherming duidelijk in een dienstverleningsovereenkomst vast te leggen, alsook voor de klant één enkele persoon als hoofdcontactpersoon en "verantwoordelijke" aan te stellen.

Bron: Artikel 37, lid 6 van de algemene verordening gegevensbescherming

8 Over welke professionele kwaliteiten moet de functionaris voor gegevensbescherming beschikken?

De functionaris voor gegevensbescherming 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 om zijn/haar taken te vervullen.

Het vereiste niveau van deskundigheid dient te worden bepaald op grond van de uitgevoerde gegevensverwerkingsactiviteiten en de bescherming die voor de verwerkte gegevens vereist is. Bijvoorbeeld: bij een bijzonder complexe dataverwerkingsactiviteit of bij verwerking van een groot aantal gevoelige gegevens kan van de functionaris voor gegevensbescherming een hoger niveau van deskundigheid en support vereist worden.

De relevante vaardigheden en deskundigheid omvatten:

- expertise in nationale en Europese wetten en praktijken inzake gegevensbescherming, met inbegrip van een grondig inzicht in de algemene verordening gegevensbescherming
- inzicht in de uitgevoerde verwerkingen
- kennis van informatietechnologieën en gegevensbeveiliging
- kennis van de bedrijfstak en de organisatie
- vermogen om binnen de organisatie een cultuur van gegevensbescherming te bevorderen

Bron: Artikel 37, lid 5 van de algemene verordening gegevensbescherming

Positie van de functionaris voor gegevensbescherming

9 Welke middelen moet de verwerkingsverantwoordelijke of de verwerker aan de functionaris voor gegevensbescherming verschaffen?

De functionaris voor gegevensbescherming moet over de nodige middelen beschikken om zijn/haar taken te kunnen uitvoeren.

Naargelang van de aard van de verwerkingen alsook de activiteiten en omvang van de organisatie moeten aan de functionaris voor gegevensbescherming de volgende middelen ter beschikking worden gesteld:

- Actieve ondersteuning van de functie van functionaris voor gegevensbescherming door het hogere management
- Voldoende tijd voor de functionarissen voor gegevensbescherming om hun taken te vervullen
- Adequate ondersteuning op het vlak van financiële middelen, infrastructuur (kantoren, faciliteiten, apparatuur) en personeel waar van toepassing
- Officiële bekendmaking van de aanstelling van de functionaris voor gegevensbescherming aan alle personeelsleden
- Toegang tot andere diensten binnen de organisatie, zodat de functionarissen voor gegevensbescherming van die andere diensten de benodigde essentiële ondersteuning, bijstand of informatie kunnen ontvangen
- Voortgezette opleiding

Bron: Artikel 38, lid 2 van de algemene verordening gegevensbescherming

10 Over welke waarborgen beschikt de functionaris voor gegevensbescherming om zijn/haar taken onafhankelijk te kunnen uitvoeren? Wat betekent "belangenconflict"?

Er bestaan meerdere waarborgen die de functionaris voor gegevensbescherming in staat moeten stellen om onafhankelijk te handelen:

- Geen instructies door de verwerkingsverantwoordelijken of verwerkers met betrekking tot de uitoefening van de taken van de functionaris voor gegevensbescherming
- Geen ontslag of sancties door de verwerkingsverantwoordelijke voor de uitvoering van de taken van de functionaris voor gegevensbescherming
- Geen belangenconflict met andere mogelijke taken en verplichtingen

De andere taken en verplichtingen van een functionaris voor gegevensbescherming mogen niet tot een belangenconflict leiden. Dit betekent in eerste instantie dat de functionaris voor gegevensbescherming binnen de organisatie geen functie kan bekleden waarbij hij of zij de doelstellingen van en de

middelen voor de verwerking van persoonsgegevens moet bepalen. Gezien de specifieke organisatiestructuur van elke organisatie moet dit geval per geval worden beoordeeld.

Als vuistregel worden binnen de organisatie als functies met een belangenconflict beschouwd: functies in het hogere management (bv. Chief Executive, Chief Operating, Chief Financial, Chief Medical Officer, hoofd van de marketingafdeling, hoofd van Human Resources of hoofd van de IT-afdeling), maar ook lagere functies binnen de organisatiestructuur als deze personen de doelstellingen van en middelen voor de verwerking van gegevens moeten bepalen. Daarenboven kan een belangenconflict zich bijvoorbeeld ook voordoen wanneer aan een externe functionaris voor gegevensbescherming wordt gevraagd om de verwerkingsverantwoordelijke of de verwerker te vertegenwoordigen in de rechtbank bij rechtszaken over problemen met de gegevensbescherming.

Bron: Artikel 38, lid 3, en artikel 38, lid 6, van de algemene verordening gegevensbescherming

Taken van de functionaris voor gegevensbescherming

11 Wat betekent "controle op naleving"?

In het kader van de taken met betrekking tot de controle op de naleving moeten functionarissen voor gegevensbescherming met name:

- informatie verzamelen om verwerkingsactiviteiten te identificeren;
- de naleving van verwerkingsactiviteiten analyseren en controleren;
- de verwerkingsverantwoordelijke of de verwerker informeren, adviseren en aanbevelingen doen.

Bron: Artikel 39, lid 1, onder b), van de algemene verordening gegevensbescherming

12 Is de DPO persoonlijk verantwoordelijk voor de niet-naleving van de vereisten inzake gegevensbescherming?

Neen. Functionarissen voor gegevensbescherming zijn niet persoonlijk verantwoordelijk voor de niet-naleving van de vereisten inzake gegevensbescherming. Het is de verwerkingsverantwoordelijke of de verwerker die moet verzekeren en kunnen aantonen dat de verwerking in overeenstemming met deze verordening is uitgevoerd. Naleving inzake gegevensbescherming behoort tot de verantwoordelijkheid van de verwerkingsverantwoordelijke of de verwerker.

13 Welke rol speelt de functionaris voor gegevensbescherming bij de gegevensbeschermingseffectbeoordelingen en de registers van de verwerkingsactiviteiten?

Voor de gegevensbeschermingseffectbeoordeling moet de verwerkingsverantwoordelijke of de verwerker aan de functionaris voor gegevensbescherming advies vragen in onder andere de volgende situaties:

- of er al dan niet een gegevensbeschermingseffectbeoordeling moet worden uitgevoerd;
- welke methodologie bij een gegevensbeschermingseffectbeoordeling moet worden gevolgd;
- of de gegevensbeschermingseffectbeoordeling intern uitgevoerd of uitbesteed moet worden;
- welke waarborgen (waaronder technische en organisatorische maatregelen) moeten worden toegepast om eventuele risico's voor de rechten en belangen van de betrokkenen te beperken;
- of de gegevensbeschermingseffectbeoordeling al dan niet correct is uitgevoerd en of de conclusies (de verwerking al dan niet uitvoeren en welke waarborgen toepassen) al dan niet in overeenstemming zijn met de vereisten inzake gegevensbescherming.

Wat de registers van de verwerkingsactiviteiten betreft, is het de verwerkingsverantwoordelijke of de verwerker en niet de functionaris voor gegevensbescherming die dergelijke registers moet bijhouden. Niets weerhoudt de verwerkingsverantwoordelijke of de verwerker er echter van om de functionaris voor gegevensbescherming te belasten met het bijhouden van de registers van de verwerkingsactiviteiten, onder toezicht van de verwerkingsverantwoordelijke of de verwerker. Dergelijke registers moeten worden beschouwd als een van de hulpmiddelen voor de functionaris voor gegevensbescherming om zijn taken uit te voeren, met name toezien op de naleving, alsook informatie verlenen aan en adviseren van de verwerkingsverantwoordelijke of de verwerker.

Bron: Artikel 39, lid 1, onder c), en artikel 30 van de algemene verordening gegevensbescherming

Gedaan te Brussel, 13 december 2016

Namens de werkgroep
De voorzitster

Isabelle FALQUE-PIERROTIN

Laatstelijk herzien en goedgekeurd op 5 april 2017

Namens de werkgroep
De voorzitster

Isabelle FALQUE-PIERROTIN