WP243 BIJLAGE - VEELGESTELDE VRAGEN

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 om een functionaris voor gegevensbescherming (Data Protection Officer, DPO) aan te stellen.

Aanstelling van de DPO (artikel 37)

1 Welke organisaties moeten een DPO aanstellen? (artikel 37, lid 1)

De algemene verordening gegevensbescherming vereist de aanwijzing van een DPO in drie specifieke gevallen:

- wanneer de verwerking door een overheidsinstantie of overheidsorgaan wordt verricht (ongeacht het type gegevens dat wordt verwerkt);
- wanneer de kerntaken van de voor de verwerking verantwoordelijke of de verwerker bestaan uit verwerkingen die regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen; en
- wanneer de kerntaken van de voor de verwerking verantwoordelijke of de verwerker bestaan uit grootschalige verwerking van bijzondere 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. En tot slot: wanneer de algemene verordening gegevensbescherming niet specifiek de aanstelling van een DPO vereist, kunnen organisaties het mogelijk wel interessant vinden om op vrijwillige basis een DPO aan te wijzen. De Groep gegevensbescherming artikel 29 ("WP29") moedigt deze vrijwillige inspanningen aan.

Voor meer informatie: zie punt 2.1 van de richtlijnen.

2 Wat betekent de term "kerntaken"? (artikel 37, lid 1, onder b) en c))

"Kerntaken" kunnen worden beschouwd als de belangrijkste handelingen die gesteld worden met het oog op het bereiken van de doelstellingen van de voor de verwerking verantwoordelijke of de verwerker. Deze omvatten ook alle activiteiten waarbij het verwerken van gegevens onlosmakelijk deel uitmaakt van de activiteit van de voor de verwerking verantwoordelijke of de verwerker. Zo moet de verwerking van medische gegevens, zoals medische dossiers van patiënten, beschouwd worden als een van de kerntaken van eender welk ziekenhuis; m.a.w.: ziekenhuizen moeten DPO's aanstellen.

Anderzijds voeren alle organisaties ondersteunende activiteiten uit, bijvoorbeeld met het oog op de uitbetaling van hun werknemers, of standaardactiviteiten ter ondersteuning van IT-infrastructuren. Dit zijn 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.

Voor meer informatie: zie punt 2.1.2 van de richtlijnen.

3 Wat betekent de term "grootschalig"? (artikel 37, lid 1, onder b) en c))

In de algemene verordening gegevensbescherming wordt niet gedefinieerd wat precies wordt bedoeld met "grootschalig". 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 grootschalige verwerking:

- verwerking van patiëntgegevens in het kader van de regelmatige bedrijfsvoering van een ziekenhuis
- verwerking van reisgegevens van individuen die gebruikmaken van het openbaar vervoerssysteem in een stad (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) door 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

Voor meer informatie: zie punt 2.1.3 van de richtlijnen.

4 Wat betekent het begrip "regelmatige en stelselmatige observatie"? (Artikel 37, lid 1, onder b))

Het begrip "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 de onlineomgeving.

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

Voorbeelden: een telecommunicatienetwerk beheren; telecommunicatiediensten leveren; retargeting via e-mail; profilering en scores toekennen met het oog op risicobeoordeling (bv. voor toekenning van een kredietscore, 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.

Voor meer informatie: zie punt 2.1.4 van de richtlijnen.

5 Kunnen organisaties gezamenlijk een DPO aanstellen? Zo ja, onder welke voorwaarden? (Artikel 37, lid 2 en 3)

In de algemene verordening gegevensbescherming wordt bepaald dat een concern één enkele functionaris voor gegevensbescherming kan aanstellen, op voorwaarde dat deze persoon "*vanuit elke vestiging makkelijk te contacteren is*". De notie van bereikbaarheid verwijst naar de taken van de DPO als contactpersoon voor de betrokkenen, de toezichthoudende autoriteit alsook binnen de organisatie. Om te verzekeren dat de DPO, hetzij intern, hetzij extern, bereikbaar is, moet vooral worden verzekerd dat diens contactgegevens in overeenstemming met de algemene verordening gegevensbescherming beschikbaar zijn. De DPO moet 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 persoonlijke beschikbaarheid van een DPO (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 DPO contact kunnen opnemen.

Voor meer informatie: zie punt 2.3 van de richtlijnen.

6 Kan er een externe DPO worden aangesteld (artikel 37, lid 6)?

Ja. Volgens artikel 37, lid 6 kan de functionaris voor gegevensbescherming een personeelslid van de voor de verwerking verantwoordelijke of de verwerker zijn (interne DPO), of kan hij/zij "de taken op grond van een dienstverleningsovereenkomst verrichten". Dat betekent dat de DPO ook een derde kan zijn die zijn/haar functie uitoefent op basis van een dienstverleningsovereenkomst die met een individu of een organisatie werd afgesloten.

Als de DPO een derde is, gelden alle vereisten van de artikelen 37 tot 39 voor deze functionaris. Wanneer de functie van DPO door een externe dienstverlener wordt bekleed, zoals in de richtlijnen vermeld, kan een team van personen die voor die entiteit werken feitelijk alle DPO-taken als team uitvoeren, onder de verantwoordelijkheid van een aangestelde hoofdcontactpersoon en "verantwoordelijke" van de klant. In dit geval is het van essentieel belang dat alle leden van de externe organisatie die de DPO-taken op zich nemen, aan alle relevante eisen van de algemene verordening gegevensbescherming voldoen.

Met het oog op juridische transparantie en goede organisatie wordt in de richtlijnen aangeraden om de taken binnen het externe DPO-team in de dienstverleningsovereenkomst duidelijk vast te leggen, alsook één enkele persoon als hoofdcontactpersoon en "verantwoordelijke" van de klant aan te duiden.

Voor meer informatie: zie punten 2.3, 2.4 en 3.5 van de richtlijnen.

7 Over welke professionele kwaliteiten moet de DPO beschikken (artikel 37, lid 5)?

Krachtens de algemene verordening gegevensbescherming moet de functionaris voor gegevensbescherming "*aangewezen worden 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*".

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. Bijvoorbeeld: bij een bijzonder complexe dataverwerkingsactiviteit of bij verwerking van een groot aantal gevoelige gegevens kan van de DPO een hoger niveau van deskundigheid en ondersteuning worden vereist.

De noodzakelijke 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

Voor meer informatie: zie punt 2.4 van de richtlijnen.

Positie van de DPO (artikel 38)

8 Over welke middelen moet de DPO beschikken om zijn/haar taken te kunnen uitvoeren?

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"*.

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

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

Voor meer informatie: zie punt 3.2 van de richtlijnen.

9 Over welke waarborgen beschikt de DPO om zijn/haar taken onafhankelijk te kunnen uitvoeren (artikel 38, lid 3)?

Er bestaan meerdere waarborgen die de DPO in staat moeten stellen om onafhankelijk te handelen zoals in overweging 97 vermeld:

- geen instructies door de voor de verwerking verantwoordelijken of verwerkers met betrekking tot de uitoefening van de taken van de DPO
- geen afwijzing of boete door de voor de verwerking verantwoordelijke met betrekking tot de uitvoering van de taken van de DPO
- geen belangenconflict met andere mogelijke taken en verplichtingen

Voor meer informatie: zie punten 3.3 tot 3.5 van de richtlijnen.

10 Welke "andere taken en verplichtingen" van een DPO zouden tot een belangenconflict kunnen leiden (artikel 38, lid 6)?

De DPO kan binnen de organisatie geen functie bekleden waarbij hij of zij de doelstellingen 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 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 en middelen voor de verwerking van gegevens moeten bepalen.

Voor meer informatie: zie punt 3.5 van de richtlijnen.

Taken van de DPO (artikel 39)

11 Wat omvat het begrip "toezicht op naleving" van de algemene verordening gegevensbescherming (artikel 39, lid 1, onder b)?

In het kader van de taken met betrekking tot het toezicht van de naleving kunnen DPO's met name:

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

Voor meer informatie: zie punt 4.1 van de richtlijnen.

12 Is de DPO persoonlijk verantwoordelijk voor de niet-naleving van de algemene verordening gegevensbescherming?

Neen, DPO's zijn persoonlijk verantwoordelijk voor de niet-naleving van de algemene verordening gegevensbescherming. In de algemene verordening gegevensbescherming staat duidelijk dat het de voor de verwerking verantwoordelijke of de verwerker is die moet verzekeren en kunnen aantonen dat de verwerking in overeenstemming met deze verordening is uitgevoerd (artikel 24, lid 1). Naleving inzake gegevensbescherming behoort tot de verantwoordelijkheid van de voor de verwerking verantwoordelijke of de verwerker.

13 Welke rol speelt de DPO bij de gegevensbeschermingseffectbeoordeling (artikel 37, lid 1, onder c)) en het register van de verwerkingsactiviteiten (artikel 30)?

Voor de gegevensbeschermingseffectbeoordeling moet de voor de verwerking verantwoordelijke of de verwerker aan de DPO 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 moet worden gevoerd of uitbesteed;
- welke waarborgen (waaronder technische en organisatorische maatregelen) moeten worden toegepast om eventuele risico's voor de rechten en belangen van te 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.

Voor meer informatie: zie punt 4.2 van de richtlijnen.

Wat het register van de verwerkingsactiviteiten betreft, is het de voor de verwerking verantwoordelijke of de verwerker en niet de DPO die een dergelijk register moet bijhouden. Maar niets weerhoudt de voor de verwerking verantwoordelijke of de verwerker ervan om de DPO te belasten met het bijhouden van het register van de verwerkingsactiviteiten, onder toezicht van de voor de verwerking verantwoordelijke. Een dergelijk register moet worden beschouwd als een van de hulpmiddelen voor de DPO om zijn taken uit te voeren, namelijk name toezien op de naleving, informatie verlenen aan en adviseren van de voor de verwerking verantwoordelijke of de verwerker.

Voor meer informatie: zie punt 4.4 van de richtlijnen.