NOTA TER VOORBEREIDING VAN DE BEGELEIDINGSCOMMISSIE VOOR DE CIVIELE VEILIGHEID

DATUM VERGADERING: 9 mei 2018

AGENDAPUNT: Aanwijzing van een data protection officer (DPO)

INDIENER:

Contactpersoon:
naam : Sandra Schroos
tel:02 500 24 81
e-mail: sandra.schroos@ibz.fgov.be

VRAAG AAN DE BEGELEIDINGSCOMMISSIE

X TER INFORMATIE
O VOOR ADVIES

THEMA (W. 15.05.2007, art.16)

- **O 1° de berekening van de meerkost voor de zone die het gevolg kan zijn van de uitvoering van de hervorming;**
- **O 2° de opdrachten die worden opgedragen aan de zones en hun financiële weerslag op de zone;**
- **O 3° de globale evaluatie van alle aspecten van de hervorming van de civiele veiligheid op lokaal niveau. Deze evaluatie bevat onder meer een monitoring van alle problemen op lokaal niveau die met de hervorming gepaard gaan.**

1. **Probleemstelling:**

Tijdens de vergadering van 21 februari 2018 vroeg de UVCW richtlijnen om te bepalen wie de zones als DPO kunnen aanstellen. Is er een bepaald profiel? Kan iemand extern worden aangeworven? Is er een risico op een belangenconflict met bepaalde functies binnen de zone? Kan 1 DPO voor verschillende zones werken?

Ter informatie vindt u hieronder een analyse, gebaseerd op:
- de AVG, hoofdstuk 4, afdeling 4 'de functionaris voor gegevensbescherming';
- de 'Guidelines on data protection officers' van de Groep Artikel 29 en
- de aanbeveling van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer (CBPL) 04/2017 betreffende de aanwijzing van een functionaris voor gegevensbescherming en in het bijzonder de toelaatbaarheid van de cumulatie van deze functie met andere functies, waaronder die van veiligheidsconsulent.

In plaats van de termen 'verwerker van gegevens' en 'verantwoordelijke voor de verwerking' wordt in deze nota omwille van de leesbaarheid de term 'overheid' gebruikt.[1] Zowel de verwerker als de verantwoordelijke voor de verwerking moeten aan de verplichtingen van de AVG voldoen en een DPO aanstellen.

[1] Volgens de Privacywet is de verantwoordelijke van de verwerking degene die het doel en de middelen voor de verwerking van de persoonsgegevens bepaalt. De verantwoordelijke hoeft de verwerking echter niet zelf uit te voeren. Hij kan hiervoor een verwerker aanstellen. Zo zal bv. een sociaal secretariaat persoonsgegevens verwerken voor een bedrijf of bestuur.

2. Oplossing + motivatie:

De AVG verplicht elke overheid, en dus elke hulpverleningszone, om een DPO te hebben en bepaalt dat 1 DPO voor verschillende overheden kan werken (art. 37, 1, a en 3). In dat laatste geval wordt verwacht dat de DPO op elk moment bereikbaar is.

De DPO kan een eigen personeelslid van de overheid zijn (in dat geval moet onderzocht worden of er geen belangenconflict ontstaat tussen de functie van DPO en de andere functie: art. 38, 6) of kan een externe zijn die wordt aangewezen via een dienstverleningscontract (art. 37, 6).

De toezichthoudende autoriteit zal de naleving van de AVG (en dus ook de verplichtingen i.v.m. de DPO) controleren. Zo zal zij o.a. nakijken of de overheid een DPO heeft aangewezen, of de DPO effectief onafhankelijk kan werken en of hij over de vereiste kwalificaties en de nodige tijd beschikt om zijn taken te vervullen. De CBPL raadt daarom aan om de analyse en de finale keuze van de aanstelling van de DPO documenteren. Bij inbreuken op de verplichtingen i.v.m. de DPO kan de toezichthoudende autoriteit geldboetes opleggen aan de overheid.

De DPO heeft minstens als opdracht om (art. 39 AVG):

- de overheid te begeleiden bij het naleven van de regels inzake gegevensbescherming (zowel de regels uit de AVG als de regels uit de nationale regelgeving en de interne regels) en de uitvoering van de essentiële elementen uit de AVG (bv. de principes van de verwerking (legaliteit, finaliteit, evenredigheid), de rechten van de personen van wie de gegevens verwerkt worden, het register, de procedure voor de melding van lekken, …) [2];
- de overheid te adviseren over de risico's van de gegevensverwerking[3];
- de overheid te adviseren over de verwerkingen die in het register moeten opgenomen worden[4];
- samen te werken met de toezichthoudende autoriteit en
- een aanspreekpunt te zijn op vlak van gegevensbescherming en dit zowel voor medewerkers, de toezichthoudende autoriteit en de personen van wie de gegevens verwerkt worden.

Bij de uitvoering van zijn taken moet de DPO rekening houden met de risico's die verbonden zijn aan de verwerking en met de aard, de omvang, de context en de doeleinden van de verwerking.

Artikel 37, 5 van de AVG beperkt zich tot de omschrijving dat de DPO wordt aangeduid 'op basis van zijn professionele kwaliteiten -inzonderheid zijn gespecialiseerde kennis van het recht en de gegevensbeschermingspraktijken- en op basis van zijn vaardigheid om zijn opdrachten te vervullen'. Er bestaat dus geen wettelijk profiel of diplomavereiste voor de DPO.

In haar aanbeveling 04/2017 stelt de CBPL dat het niveau van kennis van de DPO aangepast moet zijn aan de gevoeligheid, de complexiteit en het volume van de verwerkte gegevens. Voor de verwerking van grote hoeveelheden gevoelige gegevens zal bv. een uitgebreidere kennis nodig zijn.

In het algemeen wordt van een DPO verwacht dat hij een meer dan gemiddelde vakkennis heeft van de privacywetgeving en van de praktijk van gegevensbescherming en moet hij weten welke gegevensverwerkingen de overheid uitvoert en hoe de informatiebeveiliging geregeld is. Dit impliceert ook kennis van de werking van de overheid en de sector. Eigenlijk moet hij zorgen dat er binnen de organisatie een cultuur van gegevensbescherming kan groeien.

De CBPL sluit in haar aanbeveling niet uit dat de veiligheidsconsulent van de overheid de functie van DPO opneemt, maar benadrukt dat dit zeker geen automatisme is. De functie van DPO houdt immers veel meer in dan die van veiligheidsconsulent, die een informaticus is en op technisch vlak advies geeft over de beveiliging van gegevens, terwijl de DPO op een onafhankelijke manier moet waken over de principes van de gegevensbescherming.

De AVG voorziet verschillende maatregelen die de onafhankelijkheid van de DPO moeten garanderen (art.38):
- de DPO mag geen instructies ontvangen over de uitvoering van zijn opdrachten
- hij brengt rechtstreeks verslag uit aan de hoogste leidinggevende (de zonecommandant of de

voorzitter van de zone)
- hij heeft een geheimhoudingsplicht
- hij mag niet ontslagen worden of een sanctie krijgen als gevolg van de uitoefening van zijn taken
- hij moet aangemeld worden bij de toezichthoudende autoriteit
- hij moet binnen en buiten de overheid duidelijk geïdentificeerd zijn als DPO
- hij moet naar behoren en tijdig worden betrokken bij aangelegenheden i.v.m. de bescherming van persoonsgegevens
- hij moet de nodige middelen krijgen voor de uitvoering van zijn opdrachten
- hij mag de functie van DPO combineren met een andere functie maar er mag geen belangenconflict ontstaan.

Hoe kan een belangenconflict vermeden worden? De DPO mag niet zelf beslissen over het doel en de middelen van de gegevensverwerking en mag niet zelf de verwerking of de maatregelen voor de beveiliging uitvoeren, omdat op dat moment zijn onafhankelijkheid in gevaar komt.[5] Dit kan bijvoorbeeld het geval zijn als de DPO een managementpositie vervult zoals CEO, diensthoofd ICT, financiën, strategie, marketing of HRM, of wanneer de DPO een andere functie vervult die de doelen en middelen van de verwerking bepaalt.

De overheid zal dus moeten onderzoeken of de functie van DPO kan gecombineerd worden met een andere functie en moet idealiter de functies identificeren die onverenigbaar zijn met deze van DPO en interne regels opstellen om een belangenconflict te voorkomen.

3. Conclusie:

Samengevat heeft een DPO de volgende vaardigheden:
- juridische en technische kennis van gegevensbescherming,
- kennis van de organisatie,
- kennis van de sector en de toepasselijke regelgeving,
- menselijke capaciteiten op het vlak van communicatie en conflictbeheer,
- ethisch en integer handelen.

Afhankelijk van de omvang van de verwerking en de structuur van de overheid, kan het nodig zijn om een team te vormen rond de DPO bestaande uit verschillende profielen, elk met hun eigen vaardigheden. Zo wordt de gegevensbescherming op een overkoepelende manier benaderd. De interne structuur van het team en de taken en verantwoordelijkheden van elk lid zullen duidelijk bepaald moeten worden.[6]

Elke zone zal dus voor zichzelf moeten nagaan voor welke functies de bovenstaande omschrijving een probleem kan zijn en zal een DPO moeten aanstellen die zich, indien mogelijk, laat omringen door medewerkers die gespecialiseerd zijn op technisch en/of communicatievlak.

---

[2] De overheid (en niet de DPO) is verantwoordelijk voor de overeenstemming van de gegevensverwerking met de reglementering en riskeert de boetes.

[3] De gegevensbeschermingseffectbeoordeling zoals bedoeld in art. 35 van de GDPR. De overheid moet deze beoordeling uitvoeren, de DPO heeft enkel de taak om te adviseren over het al dan niet uitvoeren van de beoordeling, welke methode het meest geschikt is, … Indien de DPO zelf de maatregelen voor de beveiliging zou uitvoeren, is hij niet meer onafhankelijk.

[4] De overheid is zelf verantwoordelijk voor het bijhouden van het register. Indien er een verwerker werd aangesteld moeten zowel de verantwoordelijke voor de verwerking als de verwerker een register bijhouden.

[5] Artikel 38, 6 AVG en Guidelines Groep art 29.

[6] Aanbeveling 04/20017 CBPL en Guidelines Groep artikel 29.