



Aanbeveling 04/2017 van 24 mei 2017

Betreft: Aanbeveling betreffende de aanwijzing van een functionaris voor gegevensbescherming in toepassing van de Algemene Verordening Gegevensbescherming (AVG) en in het bijzonder de toelaatbaarheid van de cumulatie van deze functie met andere functies waaronder die van veiligheidsconsulent (CO-AR-2017-008)

De Commissie voor de bescherming van de persoonlijke levenssfeer ;

Gelet op de wet van *8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 30;

Gelet op het verslag van dhr. Willem Debeuckelaere ;

Brengt op 24 mei 2017 de volgende aanbeveling uit:

I. INLEIDING

1. De Algemene Verordening Gegevensbescherming (hierna AVG) is op 24 mei 2016¹ in werking getreden en zal van toepassing zijn vanaf 25 mei 2018.
2. In hoofdstuk IV van de AVG dat de verplichtingen bepaalt van de verwerkingsverantwoordelijken en de verwerkers, is afdeling IV volledig gewijd aan *de functionaris voor gegevensbescherming*. Meer in het bijzonder detailleert artikel 37 de gevallen waarin de aanwijzing van een functionaris voor gegevensbescherming verplicht is alsook de modaliteiten van deze aanwijzing; artikel 38 omkadert de functie zelf van functionaris voor gegevensbescherming (statuut) en artikel 39 beschrijft zijn opdrachten. Enkele andere artikelen van de AVG vervolledigen de omkadering van deze nieuwe functie².
3. Onmiddellijk na de goedkeuring van de AVG hebben de gegevensbeschermingsautoriteiten de kwestie van de functionaris voor gegevensbescherming als prioritair beschouwd. Zij hebben de verwerkingsverantwoordelijken en verwerkers aangespoord om snel na te gaan of zij er al dan niet juridisch toe gehouden waren een functionaris voor gegevensbescherming aan te wijzen in toepassing van artikel 37.1 van de AVG alsook om over te gaan tot de aanwervingen of het programmeren van de noodzakelijke opleidingen.³ Verenigd in de Groep artikel 29 hebben zij eveneens de vrijwillige aanduiding van dergelijke functionarissen aangemoedigd en richtsnoeren voorgesteld voor gemeenschappelijke interpretatie van de relevante artikelen van de AVG alsook een aantal aanbevelingen (best practices) geformuleerd⁴.
4. Naast de recurrente kwesties waarop zij reeds heeft geantwoord via de FAQ's⁵ op haar website (en waarvoor zij zich steunt op de gemeenschappelijke interpretaties van de

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) *Publ.blad, L 119, 4.5.2016, pp. 1–88*.

² Artikel 35 betreffende de gegevensbeschermingseffectbeoordeling bepaalt dat de verwerkingsverantwoordelijke het advies inwint van de functionaris voor gegevensbescherming indien een dergelijke functionaris werd aangewezen (§2) ; artikelen 13 en 14 betreffende de mededeling aan de betrokkene: de contactgegevens van de functionaris voor gegevensbescherming moeten hem meegedeeld worden en de artikelen 33 en 34 betreffende de meldingen van inbreuken aan de toezichhoudende autoriteit en aan de betrokkene: de contactgegevens van de functionaris moeten hen worden meegedeeld.

³ Zie bijvoorbeeld het 13 stappenplan, ontwikkeld door de CBPL: <https://www.privacycommission.be/nl/nieuws/algemene-verordening-gegevensbescherming-privacycommissie-lanceert-themadossier-en>

⁴ Groep Artikel 29, Guidelines on Data Protection Officers (« DPOs »), WP 243 van 13 december 2016, herzien na openbare consultatie en goedgekeurd in zijn definitieve versie op 5 april 2017.

⁵ Rubriek FAQ op de website van de CBPL : <https://www.privacycommission.be/nl/faq-page>

voormelde Groep artikel 29), ontvangt de CBPL regelmatig de vraag of de "veiligheidsconsulent"⁶ die sommige instellingen, organismen en andere entiteiten dienen aan te duiden in toepassing van verschillende Belgische reglementeringen, de functionaris voor gegevensbescherming kan worden - onder meer vereist voor elke openbare autoriteit en organisme (37.1. van de AVG). Mag hij de functies van veiligheidsconsulent en functionaris voor gegevensbescherming cumuleren en, in voorkomend geval, onder welke voorwaarden?

5. Onderhavige aanbeveling heeft als doel de verwerkingsverantwoordelijken en de verwerkers te begeleiden bij hun analyse en keuze voor een functionaris voor gegevensbescherming in overeenstemming van de AVG (zie punt III). Gelet op de vele vragen die de CBPL ontvangt aangaande de cumul van deze functie met die van "veiligheidsconsulent" zal in onderhavige aanbeveling bijzondere maar niet exclusieve aandacht aan dit aspect worden besteed

II. VOORGESCHIEDENIS

Uitgangspunt van de functie in de richtlijn 95/46/EG: de functionaris voor gegevensbescherming

6. Artikel 18.2. van de Richtlijn 95/46/EG heeft inderdaad reeds in 1995 de functie van "functionaris voor de gegevensbescherming" ingevoerd. Concreet hebben de lidstaten op basis van deze bepaling - zonder hiertoe verplicht te zijn - via wetgevende weg kunnen bepalen dat de verantwoordelijken voor de verwerking die een functionaris voor de gegevensbescherming aanwijzen in de zin van dit artikel 18.2. vrijgesteld worden van de voorafgaande aangifte van de verwerking bij de toezichthoudende autoriteit (zijnde de aangifte bedoeld in artikel 17 van de WVP). Volgens voormeld artikel 18.2. dient deze functionaris voor gegevensbescherming zijn taken en verplichtingen onafhankelijk te vervullen en een register bij te houden van de gegevensverwerkingsactiviteiten van de verwerkingsverantwoordelijke.
7. Een zeker aantal lidstaten van de Europese Unie hebben gebruik gemaakt van deze mogelijkheid en hebben de functie van "functionaris" voor gegevensbescherming opgenomen in hun nationale wetgeving tot omzetting van de richtlijn 95/46/EG doch niet zonder hier verschillende benamingen aan te verlenen en hem bijkomende opdrachten toe te vertrouwen naast deze die zijn opgenomen in de Richtlijn 95/46/EG. Deze bijkomende opdrachten variëren overigens van de ene nationale wetgeving tot de andere.
8. Zonder dat deze opsomming exhaustief is spreekt men momenteel onder meer over « Correspondants Informatique et Liberté » (CIL) in Frankrijk, over « Chargé de la protection des données » in het Groothertogdom Luxemburg, over « Functionaris voor de

⁶ Zie de punten 9 tot 15 hierna.

gegevensbescherming » in Nederland, over « Data Protection Officer » in het Verenigd Koninkrijk, en reeds over «Functionaris voor gegevensbescherming» in de Europese instellingen.

De functie van functionaris voor gegevensbescherming en veiligheidsconsulent in het Belgisch recht

9. In het Belgisch recht werd de functie van "aangestelde voor de gegevensbescherming" ingevoerd door artikel 17bis van de Privacywet (WVP) die stelt:

De Koning stelt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer de categorieën van verwerkingen vast die specifieke risico's inhouden voor de persoonlijke rechten en vrijheden van de betrokkenen en stelt voor deze verwerkingen, eveneens op voorstel van de Commissie voor de bescherming van de persoonlijke levenssfeer, bijzondere voorwaarden vast om de rechten en de vrijheden van de betrokkenen te waarborgen.

*In het bijzonder kan hij bepalen dat de verantwoordelijke voor de verwerking, alleen of samen met andere verantwoordelijken, **een aangestelde voor de gegevensbescherming aanwijst** die op onafhankelijke wijze zorgt voor de toepassing van deze wet en van haar uitvoeringsmaatregelen.*

De Koning bepaalt bij een in Ministerraad overlegd besluit, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, het statuut van de aangestelde voor de gegevensbescherming..

10. In tegenstelling tot artikel 18.2. van de Richtlijn 95/46/EG, koppelt artikel 17bis van de Privacywet niet de begrippen « vrijstelling van aangifte » en «aangestelde voor de gegevensbescherming ».⁷ De verantwoordelijke voor de verwerking die een aangestelde voor de gegevensverwerking aanwijst wordt op generlei wijze vrijgesteld van de aangifte van de verwerkingen die hij uitvoert bij de CBPL.

Artikel 17bis van de Privacywet koppelt daarentegen de functie van "aangestelde voor de gegevensbescherming" aan de uitvoering van verwerkingen die specifieke risico's inhouden voor de persoonlijke rechten en vrijheden van de betrokkenen (1^{ste} lid).

De Belgische wetgever is ook hier afgeweken van de voorschriften van zowel voormeld artikel 18.2. als van artikel 20 van de Richtlijn 95/46/EG. Volgens deze laatste bepaling, geven de lidstaten aan welke verwerkingen mogelijk specifieke risico's voor de persoonlijke rechten en vrijheden inhouden en dragen zij er zorg voor dat zij vóór de aanvang van de verwerking

⁷ De term "aangestelde voor de gegevensbescherming" in artikel 17bis van de Privacywet verwijst naar die van "functionaris voor de gegevensbescherming" in artikel 18 § 2 van de Richtlijn 95/46/EG.

onderzocht worden (§1), met andere woorden, vormen ze het onderwerp van voorafgaande machtigingen.

11. De CPBL heeft herhaaldelijk de wens geuit dat dit in artikel 17bis van de WVP vermelde generiek koninklijk besluit zou worden goedgekeurd. Dit is echter nooit gebeurd.
12. Meerdere specifieke wetgevingen hebben niettemin voorzien in de verplichte aanwijzing van een met deze functie belaste persoon, meestal gecumuleerd met een functie van veiligheidsconsulent of -verantwoordelijke al naargelang de terminologie die werd gebruikt door de betrokken wetgeving, zonder dat, zoals reeds werd vermeld, het statuut van deze aangestelde omstandiger werd bepaald.
13. Bij wijze van, niet exhaustief voorbeeld, citeren we:
 - a. De wet betreffende het Rijksregister stelt "*Iedere openbare overheid, openbare of private instelling die de toegang tot of de mededeling van informatiegegevens van het Rijksregister verkregen heeft, wijst, al dan niet onder haar personeel, een consulent inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer aan die onder meer de functie vervult van aangestelde voor de gegevensbescherming bedoeld in artikel 17bis van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens. (...) ».*⁸
 - b. De wet van 19 mei 2010 houdende oprichting van de Kruispuntbank van de voertuigen bepaalt in haar artikel 28 dat «*Iedere dienst wijst, al dan niet onder haar personeel, een consulent inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer aan die onder meer de functie vervult van aangestelde voor de gegevensbescherming bedoeld in artikel 17bis van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens. De identiteit van deze verantwoordelijke werd meegedeeld aan het sectoraal comité en aan de beheersdienst*».
 - c. Het koninklijk besluit van 6 december 2015 **betreffende de consulenten voor de veiligheid en de bescherming van de persoonlijke levenssfeer** en aan het platform voor de veiligheid en de bescherming van de gegevens genomen ter uitvoering van de wet op het politieambt (artikel 44/3, § 1, 5^{de} lid, 3^o, en 8, en §2, 2^{de} lid.).

⁸Artikel 8 van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *B.S.*, 21 april 1984.

14. Andere wetgevingen eisen de aanwijzing van een "Veiligheidsconsulent" zonder dat ook hier een algemene en uniforme wettelijke omkadering bestaat:

- a. Bij de opmaak van de *organieke wet op de Kruispuntbank van de Sociale Zekerheid*, besteedde de wetgever bijzondere aandacht aan de beveiliging van de Kruispuntbank, haar netwerk en de persoonsgegevens die via dit netwerk worden uitgewisseld, onder meer door te voorzien in een "veiligheidsconsulent" in elke sociale instelling⁹.
- b. De *ziekenhuisreglementering* verplicht eveneens de aanwijzing in de ziekenhuizen van een "veiligheidsconsulent" die ermee is belast de verantwoordelijke voor het dagelijks beheer te adviseren over alle aspecten van de informatiebeveiliging¹⁰.
- c. Volgens de bepalingen van de Wet van 15 augustus 2012 houdende oprichting en organisatie van een federale dienstenintegrator, dient de federale dienstenintegrator alsook elke deelnemende openbare dienst een veiligheidsconsulent aan te duiden.¹¹.
- d. Ook op gewestelijk niveau bestaan dergelijke vereisten. Volgens het Vlaams decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer moet iedere instantie die een authentieke gegevensbron beheert die persoonsgegevens bevat, iedere instantie die elektronische persoonsgegevens ontvangt of uitwisselt, en iedere entiteit die overeenkomstig artikel 4, § 3, aangewezen is en persoonsgegevens verwerkt, een veiligheidsconsulent aanwijzen (artikel 9)¹².

15. Om al deze varianten te dekken zal de algemene benaming "Veiligheidsconsulent" in het vervolg van deze aanbeveling gebruikt worden. Hoewel, zoals vermeld, er geen algemeen

⁹Artikel 24 van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid). *B.S.*, 22 februari 1990. Sinds haar goedkeuring was deze wetgeving onderhevig aan talrijke wijzigingen. Een gecoördineerde en bijgewerkte versie van de wet is beschikbaar op de website van de Kruispuntbank van de Sociale Zekerheid <http://ksz-bcss.fgov.be> Zie in het bijzonder het Koninklijk besluit van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid *B.S.* 21 augustus 1993.

¹⁰Bijlage A algemene normen van toepassing op de instellingen bedoeld in het Koninklijk besluit van 23 oktober 1964 tot bepaling van de normen die door de ziekenhuizen en hun diensten moeten worden nageleefd, bepaalt: "De houder van het bestand [de verwerkingsverantwoordelijke] wijst een veiligheidsconsulent aan belast met de veiligheid van de informatie. De veiligheidsconsulent staat de verantwoordelijke voor het dagelijks beheer met raad bij inzake alle aspecten van de veiligheid van de informatie. (...)", *B.S.* 7 november 1964.

¹¹Afdeling 5: artikelen 20-23 van het Koninklijk besluit van 17 maart 2013 betreffende de veiligheidsadviseurs ingevoerd door de wet van 15 augustus 2012 houdende oprichting en organisatie van een federale dienstenintegrator, *B.S.*, 22 maart 2013.

¹² Zie eveneens: Besluit van de Vlaamse Regering van 15 mei 2009 betreffende de veiligheidsconsulenten, vermeld in artikel 9 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.

wettelijk kader bestaat, zijn de beschrijving van de functie en het statuut van de consulent inzake informatieveiligheid van het koninklijk besluit van 12 augustus 1993 (veiligheidsconsulent van de instellingen van de sociale zekerheid) evenwel gemeenschappelijk in meerdere hogervermelde teksten (koninklijk besluit betreffende de Federale dienstenintegrator, het Vlaams besluit van 15 mei 2009,...).

Volgens deze beschrijving heeft de veiligheidsconsulent een adviserende, stimulerende, documenterende en controlerende opdracht. Artikel 3 van het Koninklijk Besluit van 12 augustus 1993 vermeldt aldus:

- De informatieveiligheidsdienst wordt geleid door de veiligheidsconsulent.
- Deze dienst adviseert (via advies) aangaande alle gedefinieerde aspecten van de informatieveiligheid zoals de strategie, regels, procedures en beveiligingsmiddelen van alle soorten informatie, zowel in de transmissie- als in de verwerkingssystemen met het oog op het waarborgen van de vertrouwelijkheid, de beschikbaarheid¹³.
- De informatieveiligheidsdienst bevordert de naleving van de veiligheidsvoorschriften opgelegd door of krachtens een wets- of reglementsbeplating en het aannemen van een veiligheidsgedrag bij de personen tewerkgesteld in de instelling.
- Dezelfde dienst legt de nodige documentatie aan dienaangaande.
- Ten slotte ziet de informatieveiligheidsdienst toe op de naleving binnen de instelling van de veiligheidsvoorschriften opgelegd door of krachtens een wets- of reglementsbeplating. Alle vastgestelde inbreuken worden schriftelijk en uitsluitend aan de verantwoordelijke voor het dagelijks bestuur van de instelling meegedeeld, vergezeld van de nodige adviezen om dergelijke inbreuken in de toekomst te vermijden.
- Aangaande zijn statuut wordt de veiligheidsconsulent aangesteld na advies van het Toezichtscomité dat nagaat (artikel 4) of de betrokkenen voldoende kennis en beschikbare tijd hebben voor de goede uitvoering van hun opdracht. Het Comité gaat eveneens na of hij geen activiteiten uitoefent die onverenigbaar zijn met de opdracht. De veiligheidsconsulent kan niet van deze functie worden ontheven wegens meningen die hij uit of daden die hij stelt in het kader van de goede uitoefening van zijn functie en moet

¹³ Zie artikel 1, 9° van het voormelde koninklijk besluit van 12 augustus 1993.

onder het rechtstreeks functioneel gezag van de verantwoordelijke voor het dagelijks bestuur van de instelling geplaatst worden.¹⁴

De praktijk van de CISO

16. Zonder hiertoe steeds wettelijk verplicht te zijn hebben een groot aantal organisaties en ondernemingen trouwens een **Hoofd Informatieveiligheid** aangeduid, soms beter gekend onder de Engelse benaming *Chief Information Security Officer (CISO)*.

Nieuwe oriëntering van de AVG

17. De AVG verlaat het concept van de functionaris voor gegevensbescherming meteen relatief beperkte rol en maakt van de nieuwe "functionaris voor gegevensbescherming" een van de hoekstenen van het accountability stelsel waarop hij is gebaseerd. Ze harmoniseert zowel de terminologie als de aanduidingscriteria, het statuut en de taken van deze functionarissen voor gegevensbescherming. Volgens de AVG reikt hun rol heel wat verder dan wat voorzien is in de richtlijn 95/46/EG of van wat werd bepaald in de verschillende nationale wetgevingen ter omzetting van deze richtlijn of andere nationale sectorale wetgevingen. Tot slot, in tegenstelling tot de Richtlijn 95/46/EG beoogt de AVG eveneens de verwerkers en niet langer alleen de verwerkingsverantwoordelijken.
18. Rekening houdend met de taken die hem worden toevertrouwd, kan de functionaris voor gegevensbescherming de conformiteit met de AVG vergemakkelijken in al zijn aspecten (accountability) en een werkelijk competitiviteitsinstrument worden voor de ondernemingen.

III. DOEL VAN DE AANBEVELING

Voor wie is deze aanbeveling bedoeld?

19. Een functionaris voor gegevensbescherming aanduiden is, in een aantal opgelijste gevallen onder artikel 37.1 van de AVG, een verplichting en, in de andere gevallen een mogelijkheid, zowel voor de verwerkingsverantwoordelijken als voor de verwerkers waarop de AVG van toepassing is, behalve indien de wetgeving van een lidstaat via legale weg een verplicht geval zou toevoegen (art. 37.4.).

Meer bepaald:

- Aangezien het gaat om de openbare sector is de aanwijzing van een functionaris voor gegevensbescherming verplicht voor de openbare overheden en openbare organismen behalve bij gerechten in de uitoefening van hun rechterlijke taken (artikel 37.1.a).

¹⁴ Het betreft het Comité bedoeld in artikel 37 van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid.

- Voor de privésector is de aanwijzing van een functionaris voor gegevensbescherming facultatief behalve in de twee gevallen waarvan sprake in artikel 37.1. b) en c) van de AVG.
20. Krachtens artikel 83 van de AVG, geven inbreuken op de verplichtingen inzake de functionaris voor gegevensbescherming waaraan de verwerkingsverantwoordelijken en de verwerkers krachtens de artikelen 37, 38 en 39 zijn onderworpen, aanleiding tot administratieve geldboeten tot 10 000 000 EUR of, voor een onderneming, tot 2% van de totale wereldwijde jaaronzet in het voorgaande boekjaar, indien dit cijfer hoger is.
21. De verwerkingsverantwoordelijke of de verwerker blijven verantwoordelijk voor de overeenstemming met de reglementering inzake gegevensbescherming en moeten deze overeenstemming kunnen aantonen. De functionaris is niet verantwoordelijk voor deze overeenstemming. Het zijn eveneens de verwerkingsverantwoordelijken en de verwerkers die kunnen gestraft worden voor inbreuken tegen de AVG.

Wat is de draagwijdte en de doelstelling van deze aanbeveling?

22. Naast de specifieke kwestie die werd aangestipt in punt 4 hiervoor, luidt de meer algemene vraag te weten of de betrokken verwerkingsverantwoordelijken en verwerkers, om zich te schikken naar de AVG, de taak van functionaris voor gegevensbescherming aan de ene of andere persoon mag toevertrouwen die overigens reeds een andere functie uitoefent in de instelling, het organisme of de onderneming. Met andere woorden, mag eenzelfde persoon de functie van functionaris voor gegevensbescherming combineren met een andere (reeds bestaande) functie?
23. Of, anders geformuleerd, kan de veiligheidsconsulent van de instellingen van sociale zekerheid, van de ziekenhuizen of nog van het Rijksregister, de functionaris voor gegevensbescherming worden? Maar ook: kan de in de bank- en verzekeringssector vereiste Compliance Officer ook de functie uitoefenen van functionaris voor gegevensbescherming? En wat voor de Directeur Human Resources, de Risk manager, de verantwoordelijke van de informaticadienst of nog de persoon die zelf geïdentificeerd wordt
24. Onderhavige aanbeveling strekt er niet toe al deze vragen te beantwoorden, noch om een antwoord te bieden voor al deze scenario's noch enig ander dat zich zou kunnen aandienen in functie van de interne organisatie van de openbare overheid, het openbaar organisme of meer in het algemeen van iedere betrokken verwerkingsverantwoordelijke of verwerker.

De CBPL zal dus in deze aanbeveling niet de verenigbaarheid onderzoeken van de cumulatie van deze verschillende functies met deze van functionaris voor gegevensbescherming zoals voorzien door de AVG, noch op het gebied van de verenigbaarheid van wetteksten die in voorkomend geval de ene of andere van deze functies omkaderen, noch op het gebied van de praktische uitoefening van deze functies, die overigens kan variëren van de ene verwerkingsverantwoordelijke en verwerker tot de andere.

25. De CBPL kan zich om verschillende redenen niet op dit pad begeven:

- a. Volgens de AVG heeft de toezichthoudende autoriteit niet de bevoegdheid gekregen om de keuze van de verwerkingsverantwoordelijke of de verwerker voor een functionaris voor gegevensbescherming te valideren. In dit opzicht dient de mededeling van de contactgegevens van de functionaris voor gegevensbescherming aan de toezichthoudende autoriteit zoals voorzien in artikel 37.7 op generlei wijze beschouwd te worden als een vraag om akkoord of validatie van de DPA met betrekking tot deze aanduiding. Een dergelijke benadering zou strijdig zijn met de accountability.
- b. De nodige flexibiliteit moet overgelaten worden aan de verwerkingsverantwoordelijken en verwerkers met betrekking tot de manier waarop zij de taken en rol van elkeen in hun schoot wensen te organiseren. Een uniek organisatorisch model moet niet worden opgelegd.
- c. De CBPL moet haar volledige onafhankelijkheid bewaren met het oog op de controles die zij genoopt zou worden uit te voeren, bijvoorbeeld ingevolge klachten tegen de verwerkingsverantwoordelijke of de verwerker, of op eigen initiatief. Hebben deze verwerkingsverantwoordelijken of verwerkers een functionaris voor gegevensbescherming aangewezen zodra zij hiertoe genoopt werden? Is deze functionaris effectief onafhankelijk? Bezit hij de vereiste kwalificaties? Beschikt hij over de nodige tijd om zijn taken effectief te vervullen?

26. De CBPL acht het niettemin belangrijk aan de betrokken verwerkingsverantwoordelijken en verwerkers een aantal richtlijnen aan te reiken om hen te helpen beslissen aan wie de functie van functionaris voor gegevensbescherming kan worden toevertrouwd in naleving van de AVG. De CBPL beveelt hen in dit verband aan hun analyse en de finale keuze te documenteren.

27. Zij herinnert er ook aan dat de AVG toelaat dat een beroep wordt gedaan op een externe functionaris (artikelen 37.3 en 37.6 van de AVG)
28. Gelet evenwel op zoals reeds gezegd, het groot aantal vragen dat de CBPL ontvangt aangaande de toelaatbaarheid van de cumulatie van de functie van functionaris voor gegevensbescherming met deze van "veiligheidsconsulent" (zie supra), zal deze aanbeveling de grote verschillen tussen deze beide functies toelichten zonder echter exhaustief te zijn.

IV. DE FUNCTIONARIS VOOR GEGEVENSBESCHERMING IN DE AVG

29. Het is afgemeten aan de functie van functionaris voor gegevensbescherming zoals beschreven in de AVG dat de verwerkingsverantwoordelijke en de verwerker, die een functionaris voor gegevensbescherming wensen of dienen aan te wijzen, de cumulatiemogelijkheid met een andere functie of de overgang van de ene naar de andere functie dienen te onderzoeken.¹⁵
30. Wat de vrijwillige aanwijzing van de functionaris betreft door de verwerkingsverantwoordelijke of de verwerker, dit wordt aangemoedigd door de Groep artikel 29. Indien hij of zij als dusdanig wordt aangewezen en de naam "functionaris voor gegevensbescherming" krijgt, zullen alle vereisten van de AVG moeten nageleefd worden. De artikelen 37 tot 39 zullen op dezelfde wijze toegepast worden als wanneer de aanwijzing verplicht was.
31. In het verleden ontwikkelde de CBPL een jurisprudentie¹⁶ in toepassing waarvan zij een duidelijk onderscheid maakte tussen de functies van veiligheidsconsulent en functionaris voor gegevensbescherming, doch zonder er zich tegen te verzetten dat eenzelfde persoon deze functies zou cumuleren voor zover de wet hem de onontbeerlijke onafhankelijkheid waarborgde voor de vervulling van deze dubbele taak:

- a. *" De veiligheidsconsulent moet waken over de beveiliging van de toe passingen en de nodige technische en organisatorische maatregelen die de naleving van de vertrouwelijkheid van de gegevens moeten waarborgen alsook de toegangen controleren. Artikel 16 van de WVP verplicht immer het nemen van de passende*

¹⁵ Wat de door de reglementering vereiste functies betreft, deze blijven van toepassing zolang de wetgever de teksten in voorkomend geval niet heeft gewijzigd.

¹⁶Advies 43/2003 betreffende een ontwerp van koninklijk besluit ter uitvoering van artikel 6, § 3, van de wet van 2 juni 1998 houdende oprichting van een Informatie- en Adviescentrum inzake de schadelijke sektarische organisaties en van een Administratieve Coördinatiecél inzake de strijd tegen schadelijke sektarische organisaties. Krachtens het goedgekeurde koninklijk besluit zijn de taken van de aangestelde voor de gegevensbescherming (Hoofdstuk III - artikel 6) beperkt tot louter de aspecten inzake gegevensbescherming (koninklijk besluit van 13 juli 2006 houdende uitvoering van artikel 6 § 3 van de wet van 2 juni 1998 houdende oprichting van een Informatie- en Adviescentrum inzake de schadelijke sektarische organisaties en van een Administratieve Coördinatiecél inzake de strijd tegen schadelijke sektarische organisaties, B.S. 16 augustus 2006).

beveiligingsmaatregelen (Veiligheidsbeginsel). De noodzaak om bij iedere verwerking te waken over al de principes die de basis vormen van de bescherming van persoonsgegevens (finaliteit, proportionaliteit, rechten van de betrokkene) noopt overigens tot de invulling van een andere functie: deze van "functionaris voor de gegevensbescherming"? Zoals we hebben gezien dekt dit begrip andere bevoegdheden dan enkel de beveiliging van de gegevens maar omvat dit ook de taak om " op onafhankelijke wijze de toepassing van onderhavige wet en haar uitvoeringsbesluiten te verzekeren", wat inhoudt, naast het controleren van het passend karakter van de veiligheidsmaatregelen, het controleren van de naleving van de rechtmatigheids- en proportionaliteitsbeginselen en van het recht op toegang van de betrokkenen. Hoewel de Commissie het onderscheid tussen de beide functies gegrond acht verzet zij zich er evenwel niet tegen dat eenzelfde persoon beide functies combineert voor zover de wet hem de onontbeerlijke onafhankelijkheid waarborgt voor de vervulling van deze dubbele taak (...)".¹⁷

Deze jurisprudentie kan vandaag niet worden aangewend om in alle gevallen te besluiten dat de vandaag in dienst zijnde veiligheidsconsulent automatisch de functionaris voor gegevensbescherming van morgen wordt. Zoals reeds vermeld is het voortaan afgemeten aan de functie van functionaris voor gegevensbescherming zoals beschreven in de AVG dat dit aspect moet worden onderzocht.

32. Zonder alle verklaringen verstrekt door de Groep 29 te herhalen die de CBPL aanbeval in haar aanbeveling 06/2016, vestigt de CBPL hierna de aandacht van de verwerkingsverantwoordelijken en verwerkers op enkele van de essentiële elementen die aan de basis liggen van de functie van functionaris voor gegevensbescherming.

¹⁷ Commissie voor de Bescherming van de persoonlijke levenssfeer, advies 33/2002 van 22 augustus 2002 betreffende het ontwerp van wet houdende oprichting van het Federaal Kenniscentrum voor de Gezondheidszorg (punt 21). Zie in dezelfde lijn: Commissie voor de Bescherming van de persoonlijke levenssfeer, Advies 19/2002 van 10 juni 2002 betreffende (1) het Ontwerp van wet tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en van de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen. (2) Ontwerp van koninklijk besluit betreffende de identiteitskaarten. (3) Ontwerp van koninklijk besluit houdende overgangsmaatregelen in verband met de elektronische identiteitskaart in België en Commissie voor de Bescherming van de persoonlijke levenssfeer, advies 23/2006 van 12 juli 2006 betreffende het voorontwerp van wet betreffende de omkadering van de negatieve lijsten (punten 42 tot 44).

Welke zijn zijn taken?¹⁸

33. De functionaris voor gegevensbescherming houdt bij de uitvoering van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico voor de rechten en vrijheden van de betrokkene, en met de aard, de omvang, de context en de verwerkingsdoeleinden. Het is de risicogebaseerde benadering die werd aangenomen door de AVG die toegepast wordt op de werkzaamheden van de functionaris voor gegevensbescherming.¹⁹ De considerans 75 verduidelijkt in dit verband:

Het qua waarschijnlijkheid en ernst uiteenlopende risico voor de rechten en vrijheden van natuurlijke personen kan voortvloeien uit persoonsgegevensverwerking die kan resulteren in ernstige lichamelijke, materiële of immateriële schade, met name: (...) »

34. **De naleving van de verordening controleren** in het algemeen: artikel 39.1.b) bepaalt dat de functionaris voor gegevensbescherming ten minste de volgende taken vervult: toezien²⁰ op naleving van de verordening (m.a.w. op alle aspecten ervan, o.a. de beginselen met betrekking tot de verwerkingen - finaliteit, rechtmatigheid, proportionaliteit enz. - de rechten van de betrokkenen, de verplichtingen van de verwerkingsverantwoordelijke en de verwerker of nog de omkadering van grensoverschrijdende doorgiften...) van de andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen en de interne regels van de verwerkingsverantwoordelijke en de verwerker met betrekking tot de bescherming van persoonsgegevens met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;

Overweging 97 verduidelijkt dat de functionaris voor gegevensbescherming de verwerkingsverantwoordelijke of de verwerker zal moeten bijstaan bij het toezicht op de interne naleving van de AVG. Concreet draagt hij bij aan de uitvoering van de essentiële elementen van de verordening zoals de principes betreffende de gegevensverwerkingen (hoofdstuk II van de AVG), de rechten van de betrokkenen (hoofdstuk III van de AVG), de gegevensbescherming by design, het Register van de verwerkingsactiviteiten, de veiligheid van de verwerking en de kennisgeving en mededeling van inbreuken op persoonsgegevens (data breach) enz. (art. 39.1. b) van de AVG).

¹⁸ Artikel 39 verduidelijkt dat de vermelde taken op z'n minst moeten toevertrouwd worden aan de functionaris voor gegevensbescherming. Zie voor meer details over de taken van de functionaris voor gegevensbescherming punt 4 van de reeds geciteerde richtsnoeren van de Groep 29.

¹⁹ Men vindt deze op het risico gebaseerde benadering voor de betrokkenen terug in de norm ISO 31000 en ISO 29134. Deze risicoanalyse overstijgt ruimschoots de risico's inzake informatiebeveiliging.

²⁰ De Engelse versie gebruikt het woord "monitoring".

In dit raam kan de functionaris meer in het bijzonder de informatie verzamelen om de verwerkingsactiviteiten te identificeren, de overeenstemming van de verwerkingsactiviteiten controleren en analyseren, advies verlenen en aanbevelingen formuleren. (Art. 39.1.a) van de AVG).²¹ Globaal zou de functie van de functionaris dus veeleer moeten gezien worden als een functie inzake begeleiding, opvolging (beter weergegeven door de Engelse term « monitoring ») dan als een controlefunctie in de strikte zin van het woord.

35. **Rol inzake gegevensbeschermingseffectbeoordeling (art. 39.2.):** onder de voorwaarden van artikel 35 (1) dient de verwerkingsverantwoordelijke - en niet de functionaris voor gegevensbescherming - een gegevensbeschermingseffectbeoordeling uit te voeren (DPIA). De functionaris kan niettemin een belangrijke rol vervullen door de verwerkingsverantwoordelijke op zijn vraag bij te staan (artikelen 35.2 en 39.1.c)). De verwerkingsverantwoordelijke zal de functionaris voor gegevensbescherming onder meer advies vragen over volgende kwesties: (1) al dan niet een gegevensbeschermingseffectbeoordeling uitvoeren, (2) de te gebruiken methode voor de gegevensbeschermingseffectbeoordeling, (3) de gegevensbeschermingseffectbeoordeling intern uitvoeren of uitbesteden, (4) welke soort waarborgen toepassen om het risico voor de rechten en vrijheden van de betrokkenen te verminderen en (5) evaluatie om te bepalen of de DPIA correct werd uitgevoerd en of de conclusies conform de AVG zijn.²²
36. **Rol van de functionaris in het bijhouden van het Register van de verwerkingsactiviteiten:** krachtens artikel 30, dienen de verwerkingsverantwoordelijke en de verwerker - en niet de functionaris - "een register bij te houden van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden (art. 30.1. voor de verwerkingsverantwoordelijken) of een "register bij te houden van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht" (art. 30.2. voor de verwerkers). De functionaris voor gegevensbescherming moet worden betrokken bij het in kaart brengen van de verwerkingen.
37. De functionaris is er eveneens toe gehouden **samen te werken met de toezichhoudende autoriteit** (art. (art. 39.1. d)) en dienst te doen als contactpunt voor de kwesties met betrekking tot de verwerking, met inbegrip van de voorafgaande raadpleging bedoeld in artikel 36, en in voorkomend geval raadplegingen uit te voeren voor elk ander onderwerp

²¹ Zie punt 4.1. voor meer details over dit luik van de taken van de functionaris voor gegevensbescherming in de reeds geciteerde richtsnoeren van de Groep 29.

²² Zie voor meer details aangaande dit luik van de taken van de functionaris voor gegevensbescherming punt 4.2 van de reeds geciteerde richtsnoeren van de Groep 29.

38. De taken die toevertrouwd worden aan de functionaris voor gegevensbescherming hebben *betrekking* op de aspecten van de gegevensbescherming die behandeld worden in de AVG inclusief de veiligheid van de verwerkingen dat, naast andere, in beginsel wordt gesteld in artikel 5 § 1 f) en uitvoeriger wordt gedetailleerd in artikel 32 van de AVG.
39. De functionaris voor gegevensbescherming moet vanuit elke vestiging "makkelijk" **te contacteren** zijn (37.2. van de AVG). Hij moet met andere woorden bereikbaar zijn²³.
40. Hij moet overigens gekend zijn door de toezichthoudende autoriteit aan wie de verwerkingsverantwoordelijke of de verwerker zijn contactgegevens moeten meedelen (37.7. van de AVG)²⁴.
41. Hij moet eveneens **gekend zijn door de betrokkenen**, waaronder de medewerkers van de instelling waar hij zijn taken uitvoert.²⁵ Aangaande de vergelijking met de "veiligheidsconsulent", komt deze transparantie bovenop deze die vereist wordt in artikel 4 van het reeds geciteerde Koninklijk besluit van 12 augustus 1993.
42. Tenslotte, om hem toe te laten zijn taken naar behoren te vervullen, dienen de verwerkingsverantwoordelijke en de verwerker ervoor te zorgen dat de functionaris :
- ***Naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens***: in het algemeen erover waken dat de functionaris van bij het begin wordt geïnformeerd en geraadpleegd wat de conformiteit met de AVG zal bevorderen en onder meer een benadering zal toelaten die werkelijk gebaseerd is op gegevensbescherming door ontwerp (*privacy by design*²⁶); Vanuit eenzelfde gedachtegang werkt de "veiligheidsconsulent" nauw samen met de diensten die dit vereisen of een beroep kunnen doen op zijn tussenkomst.²⁷
 - ***Hem de benodigde middelen ter beschikking te stellen*** via: een actieve steun van de directie, het toebedelen van voldoende tijd om zijn taken uit te voeren, de toekenning van financiële middelen, infrastructuur en in voorkomend geval voldoende personeel, een officiële mededeling aan het voltallige personeel van zijn aanwijzing in de hoedanigheid van functionaris, een toegang tot andere diensten alsook een voortdurende opleiding. Al naargelang de omvang en de structuur van het organisme kan het nodig blijken een team

²³ Zie punt 2.3. van de richtlijnen van de Groep 29 over de functionaris voor gegevensbescherming.

²⁴ Zie punt 2.5.. van de richtlijnen van de Groep 29 over de functionaris voor gegevensbescherming.

²⁵ Ibidem

²⁶ Zie punt 3.1. van de richtlijnen van de Groep 29 over de functionaris voor gegevensbescherming.

²⁷ Artikel 5 van van het voormelde koninklijk besluit van 12 augustus 1993.

te vormen rond de functionaris. De interne structuur van het team alsook de taken en verantwoordelijkheden van elkeen zullen duidelijk moeten worden bepaald.²⁸ Aangaande de vergelijking met de "veiligheidsconsulent " behoort de kwestie of hij over de nodige tijd beschikt tot de bevoegdheid van het Toezichtscomité wat niet het geval zal zijn voor de functionaris voor gegevensbescherming. Voor deze laatste zullen enkel de verwerkingsverantwoordelijke of de verwerker evalueren of aan deze vereiste is voldaan. De veiligheidsconsulent dient zijn kennis op peil te houden; aangaande de functionaris voor gegevensbescherming formuleert de AVG dit onder vorm van een verplichting ten laste van de verwerkingsverantwoordelijken en de verwerkers.

- **Zijn onafhankelijkheid waarborgen** (zie infra punt 48 dat volledig is gewijd aan dit essentieel aspect van de functie).

Welk profiel moet hij bezitten? Deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de bedoelde taken te vervullen

43. De AVG stelt 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 wat meer inhoudt dan enkel het voorzien in een adequate beveiliging en de verplichtingen met betrekking tot de verplichte beveiliging, bijvoorbeeld de mededeling van inbreuken (artikelen 33 en 34 van de AVG). Geen enkel diploma noch bijzondere certificering zijn vereist.
44. In het algemeen dient het niveau van gespecialiseerde kennis bepaald te worden in functie van de uitgevoerde gegevensverwerkingsactiviteiten en de bescherming die voor de verwerkte gegevens vereist is. Zij zal dus aangepast zijn aan de gevoeligheid, de complexiteit en het volume van verwerkte gegevens, indien de verwerkingen occasionele of regelmatige doorgiften buiten de EU omvatten enz. Naast een expertiseniveau inzake gegevensbescherming is een kennis van de activiteitensector en de organisatie van de verwerkingsverantwoordelijke of de verwerker essentieel. Ten slotte dient de bekwaamheid om zijn taken uit te voeren begrepen worden als verwijzend in de eerste plaats naar de persoonlijke kwaliteiten en de kennis van de functionaris maar eveneens naar zijn positie binnen het organisme. Ethiek en integriteit zijn verbonden met de sleutelrol die hij dient te vervullen bij het bevorderen van de gegevensbeschermingscultuur in de schoot van het organisme, wat vaak menselijke capaciteiten vereist inzake communicatie en conflictbeheer.

²⁸ Zie punt 3.2. van de richtlijnen van de Groep 29 over de functionaris voor gegevensbescherming.

Zoals reeds vermeld onder punt 42 is luidens de AVG geen enkel diploma noch bijzondere certificering vereist²⁹.

45. Aangaande de veiligheidsconsulent dient het Toezichtscomité³⁰ na te gaan of hij over de vereiste kennis beschikt voor de goede uitvoering van zijn opdracht. Zoals werd vermeld in verband met de nodige tijd waarover hij dient te beschikken, is er geen tussenkomst voorzien, noch van een Comité, noch van de Commissie voor de bescherming van de persoonlijke levenssfeer om te beoordelen of de functionaris voor gegevensbescherming al dan niet over de vereiste kwaliteiten beschikt. Dit is een eerste element.
46. Ten tweede gaat de AVG verder door te eisen dat de functionaris voor gegevensbescherming over een gespecialiseerde kennis beschikt van het recht en de praktijken inzake gegevensbescherming alsook over de capaciteit om de taken bedoeld in artikel 39 uit te voeren, zoals vermeld hiervoor in punt 44, wat ruimer is dan de loutere invoering van een passende beveiliging en de verplichtingen in verband met de veiligheidsverplichting.
47. De functionaris moet echter niet alleen werken. Hij kan – en dit lijkt meestal wenselijk – steunen op bestaande deskundige diensten - zich laten omringen door een team van meerdere profielen om zo goed mogelijk zijn opdrachten te vervullen; de uitoefening van die opdrachten vereist een holistische benadering van de gegevensbescherming en bijgevolg een waaier aan diverse en gespecialiseerde vaardigheden. Het is daarom essentieel te voorzien in een duidelijke rolverdeling voor eenieder en een duidelijke identificatie van de functionaris voor gegevensbescherming als zodanig.

Welk is zijn statuut? Onafhankelijk zijn³¹

48. De effectieve onafhankelijkheid van de functionaris voor gegevensbescherming moet volgens de AVG blijken als volgt:
 - Geen instructies ontvangen met betrekking tot de uitvoering van zijn taken (38.3.): De verwerkingsverantwoordelijke en de verwerker zorgen ervoor dat de functionaris geen instructies ontvangt met betrekking tot de uitvoering van zijn taken. De onafhankelijkheid en autonomie van de functionaris bij de uitoefening van zijn taken betekent evenwel niet dat hij over beslissingsbevoegdheden beschikt die zijn in artikel 39 voorziene taken overstijgen;

²⁹ Zie punt 2.5. van de richtlijnen van de Groep 29 over de functionaris voor gegevensbescherming.

³⁰ Het gaat hier om het Sectoraal Comité sociale zekerheid en gezondheid (voor wat de veiligheid consulent binnen de sociale zekerheid betreft).

³¹ Zie punt 3.3. van de richtlijnen van de Groep 29 over de functionaris voor gegevensbescherming.

- Niet ontslagen of gestraft worden voor de uitvoering van zijn taken (38.3. van de AVG) ³²;
- Rechtstreeks verslag uitbrengen aan het hoogste niveau van de directie (38.3. van de AVG);
- Onderworpen zijn aan geheimhouding of aan een vertrouwelijkheidsverplichting (38.5. van de AVG) : deze verplichting of beroepsgeheim³³ belet de functionaris evenwel niet de toezichthoudende autoriteit te contacteren of om advies te vragen.
- Geen belangenconflict hebben (38.6. van de AVG) : in dit verband vermelden de Richtsnoeren van de Groep van het Artikel 29 dat de functionarissen andere opdrachten en taken mogen uitvoeren voor zover dit niet leidt tot belangenvermenging. Dit impliceert onder meer dat de functionaris geen functie in de schoot van het organisme kan vervullen die hem ertoe noopt de doeleinden en de middelen van de verwerking³⁴ te bepalen. In het algemeen kunnen de conflicterende functies/posities in de schoot van een onderneming directieposten omvatten (zoals directeur-generaal, hoofd exploitatie, hoofd financiën, hoofdgeneesheer, verantwoordelijke van het departement marketing, verantwoordelijke human resources of verantwoordelijke van het departement informatica), maar kunnen eveneens lagere functies in een organisatorische structuur omvatten indien deze betrekkingen toelaten de doeleinden en de middelen van een verwerking te bepalen³⁵. De rol van de functionaris voor gegevensbescherming bestaat uit advies verstrekken en begeleiden van de verwerkingsverantwoordelijke en de verwerker bij de uitvoering van de AVG, alsook de controle. Hij kan dus niet diegene zijn die de verwerkingen verricht. Hij is daarentegen diegene die de verwerkingsverantwoordelijke adviseert over de manier waarop die verwerkingen moeten worden verricht. Op dezelfde wijze is hij betrokken bij de gegevensbeschermingseffectenbeoordeling zonder daarvoor evenwel de verantwoordelijkheid te dragen (wat toekomt aan de verwerkingsverantwoordelijke), hij zal de verwerkingsverantwoordelijke of de verwerker adviseren over de beveiliging zonder zelf de noodzakelijke maatregelen uit te voeren. Indien hij dit zou doen, zou hij zich ten aanzien van zijn functie in een ontoelaatbaar belangenconflict bevinden.

³² Zie punt 3.4. van de richtlijnen van de Groep 29 over de functionaris voor gegevensbescherming.

³³ De CBPL is van mening dat dit "beroepsgeheim" niet verwant is met het beroepsgeheim waarvan sprake in artikel 458 van het Strafwetboek.

³⁴ De bepaling van de beveiligingsmaatregelen en de invoering ervan vallen onder de verwerkingsmiddelen die door de verantwoordelijke door de verwerking worden bepaald.

³⁵ Zie punt 3.5. van de richtlijnen van de Groep 29 over de functionaris voor gegevensbescherming.

49. Zonder de term "onafhankelijkheid" te vermelden, dient de veiligheidsconsulent, zoals reeds opgemerkt, volgens het koninklijk besluit van 12 augustus 1993 rechtstreeks onder het functioneel gezag van de verantwoordelijke voor het dagelijks bestuur geplaatst te worden. Hij kan niet van deze functie worden ontheven wegens meningen die hij uit of daden die hij stelt in het kader van de goede uitoefening van zijn functie. Hij mag evenmin activiteiten uitoefenen die onverenigbaar zouden kunnen zijn.

Een aantal garanties in verband met de vereiste onafhankelijkheid van de functionaris voor gegevensbescherming bestaan dus reeds krachtens het voormeld koninklijk besluit betreffende de "veiligheidsconsulenten". Het is echter in het licht van die welke vereist worden voor de uitoefening van de functie van functionaris voor gegevensbescherming zoals bepaald in de AVG dat ze zullen moeten ingevoerd worden.

V. CONCLUSIES EN AANBEVELINGEN

50. Als conclusie bij de hiervoor uiteengezette richtlijnen alsook in de documenten waarnaar voor meer details wordt verwezen, benadrukt de CBPL de volgende elementen:
- Het is afgemeten aan de vereisten van de AVG ten opzichte van de functionaris voor gegevensbescherming dat de betrokken verwerkingsverantwoordelijke of verwerker moeten afwegen of een cumulatie van deze functie met een andere functie of een automatische overgang van de ene naar een andere functie toelaatbaar is in het licht van de AVG;
 - Met betrekking van de "Veiligheidsconsulenten" in het bijzonder, is er geen enkel automatisme noch systematische overgang van deze functie naar deze van functionaris voor gegevensbescherming; enkel een onderzoek *in concreto* door de betrokken verwerkingsverantwoordelijken en verwerkers kan hen hierin begeleiden;
 - De onderhavige aanbeveling maakt duidelijk dat de opdracht van de functionaris voor gegevensbescherming betrekking hebben op alle bepalingen van de AVG, zijnde op alle aspecten van de bescherming van persoonsgegevens (wettelijkheids-, finaliteits-, en veiligheidsbeginsel; rechten van de betrokken personen; gegevensbescherming by default; activiteitenregister van de verwerkingen; omkadering van grensoverschrijdend gegevensverkeer; beveiliging van de verwerkingen; kennisgeving van inbreuken in verband met

persoonsgegevens (databreach), met inbegrip van alle aspecten inzake de beveiliging van de verwerkingen en de informatie.

De AVG somt een aantal elementen op voor het waarborgen van de onafhankelijkheid van de functionaris voor gegevensbescherming (punt 48) die door de verwerkingsverantwoordelijke en de verwerker moeten uitgevoerd worden en in het licht waarvan, in functie van de interne organisatie, zal moeten georganiseerd worden.

- o Tenslotte, aangaande de kwalificaties van de functionaris vereist de AVG dat de functionaris voor gegevensbescherming 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. Zoals hierboven al gezegd, behelzen deze opdrachten de bescherming van gegevens in al zijn juridische, technische en organisatorische aspecten. De CBPL benadrukt het belang van dergelijke holistische aanpak van de gegevensbescherming. Daarvoor zal het in de meeste gevallen noodzakelijk zijn dat hij zich omringt met medewerkers met variërende profielen en deskundigheid in een of ander meer gespecialiseerd aspect. Of hij nu alleen werkt, in een netwerk of in een team, de functionaris voor gegevensbescherming moet altijd duidelijk geïdentificeerd zijn. Deze kwalificaties en bekwaamheden zullen niet *a priori* gevalideerd worden, noch door de Commissie voor de Bescherming van de persoonlijke levenssfeer, noch door een Sectoraal/Toezichtscomité indien het concept van deze comités zou worden behouden na de organieke hervorming van de CBPL ingevolge de AVG;
- De CBPL beveelt de betrokken verwerkingsverantwoordelijken en verwerkers aan hun keuze alsook de functie van functionaris voor gegevensbescherming te documenteren. Om de overeenstemming met de verordening aan te tonen zouden zij de nodige documentatie moeten samenstellen en groeperen. De acties die worden ondernomen en de documenten die worden opgemaakt tijdens elke etappe zullen overigens regelmatig opnieuw onderzocht en geactualiseerd moeten worden om een continu gegevensbescherming te verzekeren.
- Als *best practice* beveelt de CBPL eveneens aan dat de verwerkingsverantwoordelijken en verwerkers eveneens de betrekkingen identificeren die onverenigbaar zijn met de functie van functionaris en interne regels opstellen om belangenconflicten te voorkomen. De adviserende rol en de controle (surveillance/monitoring) op de uitvoering van de AVG door

de functionaris voor gegevensbescherming moet leiden tot de identificatie van deze belangenconflicten

- Ten slotte herinnert de CBPL eraan dat de AVG voorziet in de mogelijkheid om een externe functionaris aan te wijzen in het raam van een dienstverleningscontract.

De wnd. Administrateur,

De voorzitter,

(get.) An Machtens

(get.) Willem Debeuckelaere