



CONTROLEORGaan OP DE POLITIONELE INFORMATIE

Uw referentie	Onze referentie	Bijlage(n)	Datum
	DD200018		14 april 2020

Betreft : advies uit eigen beweging betreffende de invulling van de functie van functionaris voor gegevensbescherming of DPO¹

Het Controleorgaan op de politionele informatie (hierna afgekort 'COC' of 'Controleorgaan').

Gelet op de 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 (ook gekend als de Richtlijn politie-justitie of *Law Enforcement Directive*, hierna afgekort *LED*).

Gelet op de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (BS, 5 september 2018, hierna afgekort als 'WGB').

Gelet op de wet van 3 december 2017 tot oprichting van een Gegevensbeschermingsautoriteit.

Gelet op de wet van 5 augustus 1992 op het politieambt (hierna 'WPA').

Gelet op het verslag van de heren Frank Schuermans en Koen Gorissen, leden-raadsheren in het Controleorgaan.

Verleent op 14 april 2020 het volgend advies uit eigen beweging.

I. Algemeen

1. Op heden bestaat er enige onduidelijkheid en/of wordt het COC geconfronteerd met vragen over de juiste rol van de functionaris voor gegevensbescherming (hierna *DPO*) binnen de

¹ *Data Protection Officer.*

politiediensten (hierna 'GPI'²). Hierna wordt het wettelijk kader uiteengezet, waarna een toelichting volgt bij de deskundigheid van de *DPO*, die is verankerd in dat wettelijk kader. Vervolgens wordt dieper ingegaan op de taken van de *DPO*, die eveneens bij wet zijn vastgelegd.

2. De figuur van de *DPO* is niet nieuw. Reeds ten tijde van de oude Privacyrichtlijn 1995/46³ werd aanvaard dat het aanstellen van een *DPO* de naleving van de reglementering inzake gegevensbescherming vereenvoudigt, wat, met verantwoordingsinstrumenten zoals de gegevensbeschermingseffectbeoordeling (*DPIA*)⁴ en het uitvoeren of mogelijk maken van (interne) controles, des te meer geldt onder toepassing van de huidige regelgeving.

De *DPO* is niet persoonlijk verantwoordelijk bij de niet-naleving van de bepalingen inzake gegevensbescherming. Het is de betrokken politiedienst, in haar hoedanigheid van verwerkingsverantwoordelijke of verwerker, die moet verzekeren en kunnen aantonen dat de verwerking in overeenstemming met de respectieve bepalingen is uitgevoerd. Naleving van de regels inzake gegevensbescherming behoort dus steeds tot de verantwoordelijkheid van de politiedienst zelf en in het bijzonder de leiding.

In de WGB wordt erkend dat de functionaris voor gegevensbescherming een sleutelfiguur is in het nieuwe systeem voor gegevensbeheer en worden de regels voor zijn/haar aanwijzing, positie en taken vastgelegd.

II. Wettelijk kader

3. Titel 2, hoofdstuk 4, afdeling 5 van de WGB⁵ voorziet het wettelijk kader voor de *DPO*. Die laatste wordt aangewezen op grond van zijn/haar professionele kwaliteiten en, in het bijzonder, diens deskundigheid op het gebied van de wetgeving, de praktijk inzake gegevensbescherming en zijn vermogen om volgende taken te vervullen:

- de politiediensten, de politieambtenaren en het administratief personeel die persoonsgegevens verwerken, informeren en adviseren over hun verplichtingen met betrekking tot de bescherming van persoonsgegevens;
- toezien op de naleving van de regelgeving en de interne regels van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, de bewustmaking en de opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
- op verzoek advies verstrekken met betrekking tot de gegevensbeschermingseffectbeoordeling en erop toezien dat dergelijke gegevensbeschermingseffectbeoordeling ten minste het volgende bevat:
 - 1° een algemene beschrijving van de beoogde verwerkingen;
 - 2° een beoordeling van de risico's voor de rechten en vrijheden van de betrokkenen;

² Geïntegreerde Politie – Police Intégrée

³ Richtlijn 95/46/EG E.P. en de Raad 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, 23 november 1995*).

⁴ Data Protection Impact Assessment.

⁵ Artikelen 63 t.e.m. 65

3° de beoogde maatregelen ter beperking van de risico's (de voorzorgsmaatregelen, de beveiligingsmaatregelen en de mechanismen die zijn ingesteld om de persoonsgegevens te beschermen);

- samenwerken met het Controleorgaan in het algemeen; meer specifiek treedt de *DPO* op als contactpunt ten aanzien van het Controleorgaan inzake aangelegenheden die verband houden met gegevensverwerking en dient de *DPO* te overleggen over gelijk welke aangelegenheid in dat kader; maar de wetgeving verwijst ook specifiek naar de *DPO* als contactpunt inzake de voorafgaande raadpleging alvorens persoonsgegevens in een nieuw bestand worden opgenomen wanneer uit de aard van de verwerking (nieuwe technologieën, mechanismen of procedures) of uit de gegevensbeschermingseffectbeoordeling een hoog risico voor de rechten en vrijheden van de betrokkenen blijkt.

Er rust daarbij een verantwoordingsplicht op politiediensten om aan te tonen dat de gegevensverwerking voldoet aan titel 2 GBW, met inachtneming van de rechten en legitieme belangen van de betrokkenen en de andere belanghebbenden.

III. Deskundigheid, positie en taken van de DPO

1. In verhouding zijn

4. Het niveau van deskundigheid van de *DPO* moet in relatie staan met de gevoeligheid, de complexiteit en de hoeveelheid gegevens die de dienst(en), waarvoor hij *DPO* is, verwerk(t)en.

Zo dient er bijvoorbeeld een onderscheid te worden gemaakt tussen de deskundigheid en ondersteuning die verwacht mag worden van de *DPO* van een lokale politie, ten opzichte van de deskundigheid en ondersteuning die verwacht mag worden van de *DPO* die toeziet op de toepassing van politieverdragen, en meer bepaald op de systematische of veelvuldige uitwisseling van politionele gegevens met derde landen (buiten de EU).

2. Professionele kwaliteiten

5. De professionele kwaliteiten waarover een *DPO* dient te beschikken, kunnen overeenkomstig de regelgeving in drie luiken worden ondergebracht: (1) kennis van wetgeving, (2) kennis van de praktijk en (3) het vermogen om de bij wet voorziene taken te vervullen.

2.1. Kennis van de wetgeving

6. Over de nodige deskundigheid beschikken op het gebied van wetgeving wil niet per definitie zeggen dat een DPO een bepaald diploma hoeft te hebben. Een gepaste regelmatige opleiding door middel van permanente vorming of een vorige beroepservaring waaruit duidelijk een grondige kennis van de betreffende Europese en nationale regelgeving blijkt, kan bijvoorbeeld eveneens wijzen op een gedegen kennis van gegevensbeschermingswetgeving en -reglementering. Ook hier is 'levenslang leren' een *conditio sine qua non*.

2.2. Kennis van de praktijk

7. Kennis van de persoonsgegevensstromen binnen de structuur en de organisatie van de GPI en voldoende inzicht in de uitgevoerde verwerkingsactiviteiten, de informatiesystemen en de

informatiebehoeften van de GPI op het vlak van gegevensbescherming en gegevensbeveiliging is van belang om de functie van *DPO* bij een politiedienst, toegespitst op de dienst waar die werkzaam is uiteraard, naar behoren te kunnen uitoefenen.

Een gedegen praktijkkennis veronderstelt ook dat de *DPO* bij voorkeur toch al een aantal jaren op de teller heeft staan. Het blijft een moeilijke en enigszins arbitraire oefening daar een concreet aantal jaren op te plakken.

Een minimumervaring van 2 jaar als lid van de GPI is voor het COC niettemin een aanbevolen minimale ondergrens.

2.3. Vermogen om wettelijk voorziene taken te vervullen

8. Het vermogen om de taken te vervullen die wettelijk onder de opdrachten van een *DPO* vallen, mag niet enkel worden gezien als een verwijzing naar persoonlijke vaardigheden en kennis, maar heeft ook te maken met de positie van de *DPO* binnen de organisatie. De onafhankelijkheid van de functie dient daarbij gerespecteerd te worden, en derhalve kan of mag een hiërarchische gezagsverhouding geen invloed hebben op de rol die een medewerker als *DPO* vervult (cfr. infra).

Integriteit en voldoende professionele ethiek spelen niet enkel een grote rol in de verhouding tussen het management en de *DPO*. Ook in hoede van de *DPO* zelf zijn dit belangrijke eigenschappen: een medewerker met enkele disciplinaire sancties of negatieve evaluaties op zijn palmares is niet de geschikte persoon voor deze job.

9. De *DPO* hoort vanuit die onafhankelijkheid de ruimte te krijgen om een cultuur en collectief bewustzijn van gegevensbescherming te creëren binnen de politiedienst waarvoor hij zijn *DPO*-functie uitoefent. Hij of zij moet de mogelijkheid gelaten worden om essentiële elementen van gegevensbescherming (mee) te implementeren, zoals de beginselen van gegevensverwerking, de rechten van de betrokkenen (dit kunnen politiemedewerkers zelf zijn, maar natuurlijk vooral ook burgers), het register van verwerkingsactiviteiten, melding van en communicatie over inbreuken met betrekking tot persoonsgegevens, enz ...

3. Positie van de DPO

3.1. Betrokkenheid

10. Volgens de wet moet de betrokken politiedienst de *DPO* steeds tijdig en naar behoren betrekken bij alle aangelegenheden die met de bescherming van persoonsgegevens verband houden.

In de praktijk wil dit zeggen dat een *DPO*, steeds zo vroeg mogelijk betrokken wordt bij aangelegenheden die met gegevensbescherming verband houden. Op die manier kan er vaak ad hoc worden gereageerd, kan in een vroeg stadium rekening gehouden worden met het advies van de *DPO* en wordt zo toepassing gemaakt van het '*privacy by design*' principe. Het strekt tot aanbeveling om de redenen voor het niet volgen van het advies van de *DPO* naast het verplichte motiveren ook te documenteren.

Van zodra zich een gegevensinbreuk of een ander incident in het kader van de verwerking van persoonsgegevens voordoet dient de *DPO* onmiddellijk te worden geconsulteerd.

11. Het Controleorgaan hamert niet alleen op betrokkenheid, d.w.z. dat de korpsleiding of de operationeel leidinggevenden de *DPO* tijdig en steeds moet betrekken, maar ook dat die korpsleiding de *DPO* voldoende moet steunen in het spanningsveld dat er altijd zal zijn tussen de desiderata van de operationele politieambtenaren en de noodwendigheden van dataprotectie.

3.2. Benodigde middelen

12. De betrokken politiedienst is bij wet verplicht om diens *DPO* de benodigde middelen ter beschikking te stellen voor het vervullen van zijn opdrachten en moet hem/haar toegang tot de persoonsgegevens en de verwerkingen verschaffen. Het gaat daarbij over de ondersteuning die het management aan de *DPO* geeft: afhankelijk van de grootte van een politiezone, en de gegevensverwerkingen die daar plaatsvinden, dient een *DPO* meer of minder tijd te besteden aan zijn taken als *DPO* en dienen deze de nodige prioriteit te krijgen. Men denke bijvoorbeeld aan het voorbereiden en tijdig indienen van voorafgaande *DPIA's* bij het Controleorgaan. Met het stijgend aantal gevallen waarin nieuwe technologieën in een politiezone worden ingezet die verband houden met verwerking van persoonsgegevens (het gebruik van *drones*, van *bodycam's*, e.d.m.), kan dat mogelijk meer tijd in beslag nemen in de agenda van de *DPO*. Het management dient de *DPO* de nodige ruimte te geven in zijn takenpakket om die taken tijdig en naar behoren uit te voeren.

13. Naast tijdsindeling, vergt een adequate ondersteuning vanwege het management ten aanzien van de functie van DPO ook de nodige infrastructuur, faciliteiten en toegang tot de gegevensstromen waarvan de politiediensten gebruik maken.

Concreet is het bijvoorbeeld absoluut aan te bevelen dat de *DPO* zelf rechtstreeks toegang heeft tot de A.N.G en andere relevante politionele databanken en daarvoor niet telkens afhankelijk is van andere diensten of politiemedewerkers.

14. Ten aanzien van alle medewerkers binnen de politiedienst waarvoor een DPO zijn taken vervult, dient het management transparant te zijn over de aanstelling van de DPO en de draagwijdte van de functie. Medewerkers moeten de mogelijkheid hebben om inzake

aangelegenheden betreffende gegevensverwerking (al dan niet rechtstreeks) met de *DPO* te communiceren en omgekeerd dient de *DPO* noodzakelijk toegang te hebben, niet enkel tot de hoogste leidinggevende van de politie-entiteit, maar ook tot en essentiële ondersteuning, bijstand en informatie krijgen van verschillende relevante diensten zoals HR, IT, beveiliging, enz ...

Op die manier wordt ook vermeden dat individuele politieambtenaren of CALOG-medewerkers zonder enige vorm van filter rechtstreeks het Controleorgaan bevragen of advies vragen. Medewerkers moeten ervan doordrongen zijn dat eerst de interne kanalen moeten bevroegd worden, waarin de *DPO* een cruciale rol vervult. Het is pas indien men intern geen bevredigende oplossing vindt dat, bij voorkeur via het kanaal van de *DPO*, het COC bevroegd wordt.

15. Afhankelijk van de grootte van de politiedienst is het mogelijk dat er meer dan één persoon wordt aangeduid om de taken van *DPO* te vervullen. Elkeen die dergelijke taken vervult, moet vanuit het management ook de kans krijgen om nieuwe ontwikkelingen op het vlak van gegevensbescherming op te volgen en in dat kader opleidingen kunnen en moeten volgen om het niveau van deskundigheid hoog en op niveau te houden.

In beginsel dient de *DPO* meer middelen ter beschikking te krijgen naarmate de complexiteit en gevoeligheid van de gegevensverwerking stijgt.

3.3. Onafhankelijkheid

16. Overeenkomstig artikel 64, lid 3 WGB dient een politiedienst erop toe te zien dat de *DPO* géén instructies ontvangt met betrekking tot de uitvoering van zijn taken als *DPO* met het oog op het verzekeren van voldoende autonomie voor de *DPO*.

Concreet heeft deze onafhankelijkheid niet enkel betrekking op het te bereiken of bereikte resultaat, maar eveneens op de manier waarop een klacht wordt behandeld, op de vraag of een *DPO* contact mag opnemen met het Controleorgaan, al dan niet in het kader van een vraag om informatie, dan wel om een melding te doen.

17. Die onafhankelijkheid geldt ongeacht de tewerkstellingsvorm waaronder de *DPO* wordt aangeworven. Zo is het vanuit integriteitsoogpunt onaanvaardbaar om een CALOG personeelslid, dat onder een contract van bepaalde duur werkzaam zou zijn, aan te stellen als *DPO*, waarbij de 'medewerking' of de 'soepelheid' in de hoedanigheid van *DPO* een stok achter de deur is of zou kunnen zijn om de tewerkstelling te verlengen, dan wel te beëindigen. De *DPO* moet in alle vrijheid en onafhankelijkheid, zonder risico voor zijn tewerkstelling of zonder enig ander nadeel, advies kunnen verlenen dat ingaat tegen het standpunt van het management. Meer nog, in lijn met wat op Europees niveau als richtlijn voor *DPO's* werd geformuleerd door de 'groep gegevensbescherming artikel 29', zou in een tewerkstellingscontract van een medewerker die de taken van *DPO* op zich neemt, een ontslag van de betrokken medewerker op basis van diens activiteiten als *DPO* (maar niet het gebrek eraan) moeten worden uitgesloten⁶.

Gelet op het feit dat een *DPO* bij de GPI een personeelslid van de politie dient te zijn (cf. verder) zullen de meeste tewerkstellingsvormen echter van statutaire aard zijn zodat de

⁶ Zie https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 p. 15.

essentie erin moet bestaan dat de DPO geen enkel nadeel mag ondervinden als gevolg van de uitoefening van zijn functie.

18. Ook andere (al dan niet subtielere) vormen van drukingsmiddelen vanuit het management dan die betreffende de tewerkstelling of loopbaan van de *DPO* zijn niet aanvaardbaar of toegelaten. Het tegenhouden of uitstellen van een promotie, mobiliteitsaanvraag of functiewijziging, het intrekken van voordelen die andere medewerkers wel genieten, de evaluatie van de *DPO* laten afhangen van de overeenstemming tussen zijn/haar advies en het standpunt van het management of het dreigen met één van deze drukingsmiddelen is vanzelfsprekend uit den boze.

De onafhankelijkheid van de *DPO* houdt geenszins in dat deze over meer beslissingsbevoegdheid zou beschikken dan voor zijn wettelijke taken is vereist: de politie en de leiding ervan blijft als verwerkingsverantwoordelijke gehouden tot naleving van de beginselen van verwerking, zoals noodzakelijkheid, proportionaliteit en doelgebondenheid en moet de naleving van die beginselen kunnen aantonen, conform artikel 29 §5 WGB. Meer bepaald ligt de beslissingsbevoegdheid steeds bij het management van de betrokken politiedienst(en) zelf, maar de *DPO* mag daarbij niet beknot worden om zijn/haar, van die beslissing afwijkende, mening te formuleren en daarover aan de korpschef/korpsleiding te rapporteren wanneer de *DPO* meent dat de beslissing die het management van de politiedienst heeft genomen in strijd is met de regelgeving inzake gegevensverwerking en -bescherming.

Idealiter stelt de *DPO* eveneens een jaarverslag op van zijn activiteiten, met zijn al dan niet afwijkende mening over de verschillende aangelegenheden die binnen het toepassingsveld van de gegevensverwerking gedurende dat jaar werden behandeld of beslist door het management. Ook dat verslag zou dan rechtstreeks aan de korpschef worden overgemaakt en ter beschikking zijn van het Controleorgaan.

3.4. Belangenconflicten

19. De medewerker die als *DPO* werkzaam is bij één of meer politiediensten kan ook andere taken en plichten vervullen dan louter die van *DPO*, met uitsluiting van managementfuncties of functies waarbij de *DPO* eveneens de doelstellingen en de middelen voor de verwerking van persoonsgegevens moet of mee helpt bepalen. Het is aan de verwerkingsverantwoordelijke politiedienst en niet aan de *DPO* zelf om ervoor te zorgen dat zijn taken en plichten niet tot een belangenconflict leiden⁷.

De taakomschrijving van de *DPO* dient voldoende gepreciseerd en gedetailleerd te zijn om belangenconflicten te kunnen detecteren en vermijden.

3.5. Statuut

20. Artikel 144 Wet Geïntegreerde Politie bepaalt: "*Elke verwerkingsverantwoordelijke en minstens elke politiezone, het commissariaat-generaal, elke algemene directie en elke directie van de federale politie wijst personeelsleden van de politie⁸ als functionaris voor gegevensbescherming aan overeenkomstig artikel 37 van de algemene verordening gegevensbescherming en artikel 63 van de wet gegevensbescherming*".

⁷ Cfr. artikel 64 *in fine* WGB

⁸ Eigen onderlijning.

Het is dus duidelijk dat, voor wat de GPI betreft, de DPO hetzij een lid van het operationeel kader, hetzij een lid van het CALOG-kader moet zijn. Het is niet toegestaan een functie van DPO over te laten aan een externe dienstverlener (genre consultant, private expert, enz ...).

2. Taken van de DPO

1. Het management en het personeel informeren en adviseren over hun verplichtingen met betrekking tot de bescherming van persoonsgegevens.

21. Concreet dient een *DPO* zich in eerste instantie in zijn informatieverstrekking en advies te richten op zaken die een hoger risico voor de gegevensbescherming inhouden. Dergelijke aanpak helpt *DPO's* om de betrokken politiedienst(en) te adviseren omtrent de methode die men zou gebruiken bij het uitvoeren van een gegevensbeschermingseffectbeoordeling, de zaken die bij een nazicht van de interne gegevensbescherming moeten onderzocht worden, maar ook omtrent de interne opleidingen die aan de medewerkers of het management gegeven dienen te worden en aan welke verwerkingsactiviteiten meer en/of het meeste tijd en middelen moeten worden besteed.

2. Toezien op de naleving van de regelgeving en de interne politionele regels betreffende de bescherming van persoonsgegevens

22. In het kader van dat toezicht op de naleving van de reglementering dient de *DPO* informatie te kunnen verzamelen om verwerkingsactiviteiten te identificeren, de naleving ervan te analyseren en desgevallend aanbevelingen te doen.

Dat toezicht heeft onder meer betrekking op het beleid van de betrokken politiedienst(en) waarvoor de *DPO* werkzaam is (als *DPO*). Concreet houdt dit in dat een *DPO* de toewijzing van verantwoordelijkheden, de bewustmaking en de opleiding van het bij de verwerking betrokken personeel en de betreffende audits aanstuurt. Zo kan een *DPO* perfect aanbevelingen doen omtrent de genomen maatregelen om ervoor te zorgen dat alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor politionele verwerkingsdoeleinden, wat impliceert dat hij/zij hiervan uiteraard op de hoogte wordt gesteld teneinde zijn/haar taken als *DPO* naar behoren te kunnen vervullen. De *DPO* moet de hoeveelheid verzamelde persoonsgegevens kunnen nagaan, de mate waarin zij worden verwerkt, de periode waarin zij worden opgeslagen en de toegankelijkheid daarvan.

3. Rol betreffende de gegevensbeschermingseffectbeoordeling (*DPIA*)⁹

23. Eén van de wettelijke opdrachten van een *DPO* is om desgevraagd advies te verstrekken met betrekking tot een gegevensbeschermingseffectbeoordeling (*DPIA*). Daarbij dient de *DPO* toe te zien op de uitvoering van dergelijke beoordeling in overeenstemming met de toepasselijke wetsbepalingen.

De wet omschrijft wanneer een gegevensbeschermingseffectbeoordeling moet worden uitgevoerd¹⁰.

24. De concrete invulling van die wettelijke voorwaarden wordt hieronder nader toegelicht:

⁹ Data Protection Impact Assessment.

¹⁰ Artikel 59 WGB

- Wanneer een soort verwerking waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen oplevert

Of dergelijk hoog risico waarschijnlijk is, moet beoordeeld worden op basis van de (gevoelige) aard, de reikwijdte, de context of de doeleinden van de verwerking. Ook de waarborgen die ter bescherming van de persoonsgegevens voorhanden zijn, zijn hier van belang.

Concreet moet men rekening houden met de vraag hoe grootschalig verwerkingen worden verricht, of het om aanzienlijke hoeveelheden persoonsgegevens gaat, op welk (lokaal, regionaal, nationaal of supranationaal) niveau de verwerkingen plaatsvinden en hoe groot het aantal betrokkenen is dat (nadelige) gevolgen zou kunnen ondervinden ten gevolge van de verwerkingen.

De gevoelige aard van een verwerking kan onder meer verwijzen naar bv. een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen die is gebaseerd op de profilering van gegevens, of de verwerking van bijzondere categorieën van persoonsgegevens, biometrische gegevens of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten.

Derhalve zullen politionele gegevens in de praktijk meestal gevoelig van aard zijn.

Daarnaast is het van belang dat de betrokken politiezone(s) of diensten de risico's ter zake erken(t)/(nen) en toelichten welke beperkingen er worden ingevoerd voor de rechten en vrijheden van natuurlijke personen. Vooral wanneer natuurlijke personen hun rechten minder gemakkelijk kunnen uitoefenen, is het belangrijk dat de betrokken politiedienst voldoende motiveert waarom de verwerking van de persoonsgegevens primeert op die beperkingen of eventueel zelfs op een onmogelijkheid om bepaalde rechten uit te oefenen.

Met andere woorden betreft het hier een zelf-evaluatie op het vlak van gegevensbescherming die de betrokken politiediensten zo volledig mogelijk dienen uit te voeren, rekening houden met alle betrokkenen en hun legitieme belangen.

Een gegevensbeschermingseffectbeoordeling beperkt zich overigens niet noodzakelijk tot een enkel project, maar kan een veelheid aan doeleinden en niveaus beslaan, bv. wanneer verschillende politiediensten een gemeenschappelijke verwerkingsapplicatie of -platform willen opzetten of wanneer meerdere politiezones of diensten van plan zijn een gemeenschappelijke verwerkingsapplicatie of -omgeving in te voeren als multifunctionele tool, waardoor ook de risico's op vlak van gegevensbescherming, verbonden aan dergelijke verwerkingen, sneller toenemen en meer aandacht vereisen.

- Met bijzondere aandacht voor het gebruik van nieuwe technologieën

Men denke daarbij bijvoorbeeld aan het gebruik van *bodycam's* of *drones*, vooral wanneer deze uitgerust zijn met nog nooit eerder gebruikte of geteste software.

Hierbij moet worden gekeken naar de stand van de technologie, de gangbaarheid van bestaande technologie, de nieuwe gebruiksmogelijkheden die worden toegevoegd aan bestaande *software*, e.d.m. Wanneer het bv. om een pilootproject gaat waarbij reeds bestaande technologie voor het eerst binnen een politiedienst wordt ingezet, zonder dat de impact voor de gegevensbescherming in het verleden werd afgebakend, strekt het tot

aanbeveling om een gegevensbeschermingseffectbeoordeling ter advies voor te leggen aan de *DPO* om de beoordeling zo kwalitatief en deskundig mogelijk uit te werken.

- *Voorafgaand aan de verwerking van de gegevens*

Opdat de gegevensbeschermingseffectbeoordeling functioneel zou zijn, dient zij tijdig te gebeuren. Het volstaat niet dat er al een gegevensbeschermingseffectbeoordeling uitgevoerd werd in het kader van de vaststelling van de rechtsgrond, om vervolgens geen effectbeoordeling op te maken voor de verwerkingsactiviteiten zelf die steunen op die rechtsgrond. Ook een kopie van die beoordeling volstaat niet, nu deze hoort toegespitst te zijn op de specifieke kenmerken en gevolgen van de verwerkingsactiviteit en de praktische implementatie.

25. Opdat de *DPO* de betrokken politiedienst(en) zou kunnen ondersteunen in de opmaak van de gegevensbeschermingseffectbeoordeling, dient desgevallend de vraag om advies eveneens tijdig te gebeuren. Hoeveel tijd nodig is voor de adviesverlening kan best bepaald worden rekening houdend met de verschillende aspecten waarop zo'n beoordeling betrekking heeft, nl. op een analyse van de voorgenomen maatregelen, waarborgen en mechanismen voor het beschermen van persoonsgegevens, alsook moet men aantonen dat aan de gegevensbeschermingswetgeving is voldaan. Effectbeoordelingen dienen relevante systemen en procedures van verwerkingsactiviteiten te bestrijken, maar geen individuele gevallen.

26. Of het management desgevallend advies vraagt aan de *DPO*, mag geenszins afhangen van een opportuiniteitsbeoordeling betreffende de opstart van de verwerkingsactiviteit of de uiteenlopende standpunten die door het advies tot uiting zouden kunnen komen. Uiteraard betreft het hier een discretionaire bevoegdheid van het management, maar desalniettemin dient zij wel de regel te respecteren dat de *DPO* naar behoren wordt betrokken bij alle aangelegenheden die met de bescherming van persoonsgegevens verband houden, ook al zou zij het niet nodig achten om ter zake advies in te winnen bij de *DPO*.

4. Optreden als contactpunt voor en samenwerken met het Controleorgaan

27. Deze taak is nauw verbonden met de onafhankelijkheid die een *DPO* dient te genieten ten aanzien van de politiedienst(en) waarvoor hij actief is in zijn hoedanigheid als *DPO*: de betrokken politiedienst(en) mag/mogen niet als dusdanig oordelen of beïnvloeden wanneer de *DPO* contact opneemt met het Controleorgaan. Het gaat dan vooral over situaties waarbij de *DPO* vanuit zijn expertise op vlak van gegevensbescherming oordeelt dat het nuttig kan zijn of noodzakelijk is om het Controleorgaan in te lichten, dan wel om advies te vragen, of uitsluitel te geven over omstandigheden die mogelijks de gegevensbescherming en/of de rechten van natuurlijke personen impacteren.

Ook in het kader van de melding en documentatie van inbreuken in verband met persoonsgegevens of inbreuken op de beveiliging, de gevolgen ervan en de genomen corrigerende maatregelen speelt de *DPO* een belangrijke rol in de communicatie naar het Controleorgaan toe.

Wanneer de politiedienst een (nieuwe) *DPO* aanduidt, dient zij in haar hoedanigheid van verwerkingsverantwoordelijke de contactgegevens van de *DPO* aan het Controleorgaan mee

te delen, teneinde de goede samenwerking te bewerkstelligen en te voldoen aan haar wettelijke verplichting¹¹.

28. Tot slot kan verwezen worden naar de bevoegdheden van het Controleorgaan, bij de uitoefening waarvan de *DPO* als contactpunt op verzoek zijn volledige samenwerking en medewerking hoort te verlenen aan het COC, en dit in verbinding met, maar ook onafhankelijk van de politiedienst(en) waarvoor hij/zij actief is.

Tot slot herhalen we hier (cf. randnummer 14) dat moet worden vermeden dat individuele politieambtenaren of CALOG-medewerkers zonder enige vorm van filter rechtstreeks het Controleorgaan bevragen. Medewerkers behoren prioritair de interne kanalen te bevragen waaronder de *DPO*. Het is pas indien men intern geen bevredigende oplossing vindt dat via het kanaal van de *DPO* het COC bevroegd wordt.

De *DPO* is dus ook de bevoorrechte gesprekspartner van en voor het COC.

IV. Besluit

29. Hoewel de figuur van de *DPO* niet nieuw is, werd de functie meer en sterker wettelijk verankerd in de WBG, wat ook het belang van die functie en van de taken die een *DPO* binnen de GPI op zich neemt benadrukt.

Uitgaande van de *LED*, heeft de Belgische wetgever de nadruk gelegd op de vereiste van deskundigheid in hoofde van de *DPO* op het vlak van gegevensbescherming. Zijn expertise hoort in verhouding te staan tot de complexiteit van de gegevensverwerking waarmee hij op de werkvloer in aanraking komt, en zijn professionele kwaliteiten dienen zowel betrekking te hebben op de relevante wetgeving, de structuur en organisatie van de GPI en de politionele gegevensstromen, maar ook op persoonlijke vaardigheden en op een professionele ethiek van een hoog niveau.

30. Van primordiaal belang is de positie van de *DPO*: elke politiedienst dient de balans te vinden tussen voldoende betrokkenheid van de *DPO* bij alle aangelegenheden betreffende de verwerking van persoonsgegevens, het voorzien van de benodigde middelen om de *DPO* toe te laten zijn taken naar behoren uit te voeren en de onafhankelijkheid die een *DPO* eigen hoort te zijn in de uitoefening van die taken. Vooral de gezagsverhouding en de materiële of inhoudelijke taken die naast deze functie mogelijks bijkomend nog op de *DPO* rusten, zijn gevoelige aandachtspunten om dat delicaat evenwicht te bereiken en belangenconflicten te vermijden. Maar ook infrastructuur, tijdsbesteding en de nodige toegang tot alle relevante gegevens en (politionele) databanken zijn van belang.

31. Ten slotte is een goed begrip van de taken van een *DPO* nodig om een omvattend beeld te hebben van de functie. Daartoe dient het management in de nodige ondersteuning te voorzien. De *DPO* moet zowel het management als de politiemedewerkers waarvoor hij *DPO* is informeren en adviseren over alle aangelegenheden die betrekking hebben op de verwerking van persoonsgegevens en hij/zij ziet toe op de naleving van de regelgeving en de interne politionele regels. Zijn/haar rol bij de opmaak van een gegevensbeschermingseffectbeoordeling (*DPIA*) hangt deels af van het beleid dat het management hieromtrent heeft uitgestippeld, doch het strekt tot aanbeveling, om bij

¹¹ Cf. artikel 63, 4^e lid WGB.

gevoelige aangelegenheden en hoge risico's steeds beroep te doen op de expertise van de *DPO*. Zeker wanneer het nieuwe technologieën of complexe materies betreft, kan het advies van de *DPO* bijdragen tot een betere inschatting van de waarschijnlijkheid van de risico's en/of tot een beter overzicht inzake gegevensverwerking voor het management.

Tenslotte is de goede medewerking, samenwerking en communicatie met het Controleorgaan eveneens een belangrijke taak voor de *DPO*, nu hij/zij steeds als eerste aanspreekpunt fungeert en er geen drempelvrees mag bestaan om relevante meldingen te doen aangaande gegevensbeschermingsproblemen of inbreuken dienaangaande.

Het is van belang elke wijziging van *DPO* dadelijk mee te delen aan het Controleorgaan.

**Om deze redenen,
het Controleorgaan op de politionele informatie,
verleent uit eigen beweging voorliggend advies**

Geeft overeenkomstig artikel 237, tweede, derde en vierde lid WGB kennis van dit ambtshalve advies aan:

- de Ministers van Veiligheid en Binnenlandse Zaken en Justitie
- het College van procureurs-generaal
- de Commissaris-generaal van de federale politie
- de Vaste Commissie van de Lokale Politie

Advies uit eigen beweging goedgekeurd door het Controleorgaan op de Politionele Informatie op 14 april 2020

Voor het Controleorgaan,

De voorzitter,

(get.) Philippe ARNOULD