CONTROLEORGAAN OP DE POLITIONELE INFORMATIE

Uw referentie	Onze referentie	Bijlage(n)	Datum
	DA200007		22/09/2020

<u>Betreft</u>: Advies betreffende een Gemeenschappelijke dwingende richtlijn van de Ministers van Justitie en van Binnenlandse Zaken met betrekking tot de maatregelen die nodig zijn om het beheer en de veiligheid, waaronder in het bijzonder de aspecten met betrekking tot de betrouwbaarheid, de vertrouwelijkheid, de beschikbaarheid, de traceerbaarheid en de integriteit van de persoonsgegevens en de informatie die worden verwerkt in de gegevensbanken bedoeld in artikel 44/2 van de Wet op het Politieambt, te verzekeren (richtlijn informatieveiligheid).

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

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'), artikel 71 en Titel VII, inzonderheid artikel 236.

Gelet op de wet van 3 december 2017 tot oprichting van een Gegevensbeschermingsautoriteit (hierna afgekort "WOG").

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

Gelet op de wet van 7 december 1998 tot organisatie van een geïntegreerde politie, gestructureerd op twee niveaus (hierna 'WGP').

Gelet op de '*Law Enforcement Directive'* 2016/680 van 27 april 2016 (hierna *LED*).

Gelet op de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens.

Gelet op het verzoek van adviseur S. Godin (Technisch en Administratief Secretariaat Geïntegreerde Politie bij het kabinet Justitie) namens de Minister van Justitie en de Minister van Veiligheid en Binnenlandse zaken van 17 september 2020 ontvangen per elektronische bericht door het Controleorgaan, op grond van voormelde WGB om een advies uit te brengen.

Gelet op het verslag van de heer Frank Schuermans, lid-raadsheer in het Controleorgaan.

Brengt op 22 september 2020 het volgend advies uit.

I. Voorafgaande opmerking nopens de bevoegdheid van het Controleorgaan

1. In het licht van, respectievelijk, de toepassing en omzetting van de Verordening 2016/679[1] en de Richtlijn 2016/680[2] heeft de wetgever de taken en opdrachten van het Controleorgaan grondig gewijzigd. Artikel 4 § 2, vierde lid van de WOG bepaalt dat de competenties, taken en bevoegdheden als toezichthoudende autoriteit voorzien door de Verordening 2016/679 voor de politiediensten in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie, gestructureerd op twee niveaus, worden uitgeoefend door het Controleorgaan.

2. Het Controleorgaan moet geraadpleegd worden bij de voorbereiding van wetgeving of een regelgevende maatregel die verband houdt met de verwerking van persoonsgegevens door de politiediensten van de geïntegreerde politie (zie artikel 59 §1, 2e lid en 236 §2 WGB, artikel 36.4 van de AVG en artikel 28.2 van de Richtlijn politie-justitie of *LED*). Daarbij heeft het Controleorgaan de opdracht om te onderzoeken of de voorgenomen verwerkingsactiviteit door de politiediensten in overeenstemming is met de bepalingen van Titel 1 (voor de niet-operationele verwerkingen)[3] en Titel 2 (voor de operationele verwerkingen) van de WGB[4]. Wat betreft derhalve in het bijzonder de verwerkingsactiviteiten in het kader van de opdrachten van bestuurlijke en/of gerechtelijke politie brengt het Controleorgaan advies uit, hetzij uit eigen beweging, hetzij op verzoek van de Regering of van de Kamer van volksvertegenwoordigers, van een bestuurlijke of gerechtelijke overheid of van een politiedienst, inzake iedere aangelegenheid die betrekking heeft op het politionele informatiebeheer zoals geregeld in Afdeling 12 van Hoofdstuk 4 van de wet op het politieambt[5].

3. Het Controleorgaan is, ten aanzien van de politiediensten, de Algemene Inspectie van de federale politie en lokale politie (afgekort 'AIG') zoals bedoeld in de wet van 15 mei 2007 op de Algemene Inspectie en de Passagiersinformatie-eenheid (hierna afgekort 'BEL-PIU') bedoeld in Hoofdstuk 7 van de wet van 25 december 2016 tevens belast met het toezicht op de toepassing van Titel 2 van de GBW en/of de verwerking van persoonsgegevens zoals bedoeld in de artikelen 44/1 tot 44/11/13 van de wet op het politieambt en/of elke andere opdracht die haar krachtens of door andere wetten wordt verleend.[6]

---

[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 of 'AVG').

[2] 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 (hierna 'Richtlijn politie-justitie' of *LED*).

[3] Artikel 4 §2, vierde lid WOG.

[4] Artikel 71 §1, derde lid WGB.

[5] Artikelen 59 §1, 2e lid en 236 § 2 WGB.

[6] Artikel 71 §1, derde lid juncto 236 § 3, WGB.

4. Het Controleorgaan is tot slot ingevolge artikel 281, § 4, van de algemene wet van 18 juli 1977 "*inzake douane en accijnzen*", zoals gewijzigd door de wet van 2 mei 2019 "*tot wijziging van diverse bepalingen met betrekking tot de verwerking van passagiersgegevens*" ten aanzien van de Dienst Geschillen van de Algemene Administratie van Douane en Accijnzen bevoegd in het kader van de vorderingen gericht aan de BELPIU in fiscale materies.

II. VOORWERP VAN DE AANVRAAG

5. Het voorwerp van de aanvraag wordt door de aanvragers als volgt omschreven:

"Par le présent mail, les cabinets de l'Intérieur et de la Justice souhaitent vous soumettre pour avis 4 projets de directive commune des Ministres de la Justice et de l'Intérieur qui viennent compléter l'arsenal juridique en matière de gestion d'information policière opérationnelle. Ces directives trouvent leur fondement juridique dans les articles suivants de la loi sur la fonction de police :

(i) L'article 44/4, §2 (*Directive sur les mesures nécessaires en vue d'assurer la gestion et les mesures de sécurité des données à caractère personnel et des informations traitées dans les banques de données visées à l'article 44/2*)

(ii) L'article 44/4, §§ 3 et 5 (*Directive sur l'accès à la B.N.G., aux banques de données de base, aux banque de données particulières, et aux banques de données techniques par les membres du personnel des services de police)*

(iii) L'article 44/4, §§ 4 et 5 (*Directive sur l'interconnexion des banques de données visées à l'article 44/2 entre elles ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique*)

(iv) L'article 44/4, § 6 de la LFP (*Directive sur l'interconnexion ou la corrélation des banques de données* techniques)

Nous vous envoyons également pour avis le projet de fiche CO2 de la MFO3 concernant les mesures à prendre vu le lien de cette fiche avec les interconnexions et corrélations opérées dans des banques de données techniques. Comme vous le savez, deux de ces directives devront être publiées au Moniteur belge, à savoir, (i) la directive sur à l' accès à la B.N.G., aux banques de données de base, aux banque de données particulières, et aux banques de données techniques par les membres du personnel et (ii) celle sur l'interconnexion des banques de données visées à l'article 44/2 entre elles ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique[7] ».

---

[7] Vrije vertaling: "Met deze mail wensen de kabinetten Binnenlandse Zaken en Justitie u 4 ontwerpen van richtlijn, die het juridisch arsenaal met betrekking tot de politionele operationele informatiehuishouding vervolledigen, voor advies voor te leggen. Deze richtlijnen vinden hun rechtsgrondslag in de volgende artikelen van de wet op het politieambt:

(i) Artikel 44/4 §2 (Richtlijn met betrekking tot de maatregelen die nodig zijn om het beheer en de veiligheid van de persoonsgegevens en de informatie die worden verwerkt in de gegevensbanken bedoeld in artikel 44/2)

(ii) Artikel 44/4 §§ 3 et 5 (Richtlijn met betrekking tot de toegang tot de ANG, de basisgegevensbanken, de bijzondere gegevensbanken en de technische door de leden van de politiediensten)

Voor de leesbaarheid zal het COC voor elk van de voormelde richtlijnen de volgende afkortingen gebruiken:

(i) Artikel 44/4 §2 (Richtlijn met betrekking tot de maatregelen die nodig zijn om het beheer en de veiligheid van de persoonsgegevens en de informatie die worden verwerkt in de gegevensbanken bedoeld in artikel 44/2): "**Richtlijn informatieveiligheid**"
(ii) Artikel 44/4 §§ 3 et 5 (Richtlijn met betrekking tot de toegang tot de ANG, de basisgegevensbanken, de bijzondere gegevensbanken en de technische door de leden van de politiediensten): "**Richtlijn toegangsregels**"
(iii) Artikel 44/4 §§ 4 et 5 (Richtlijn betreffende de koppeling van de gegevensbanken bedoeld in artikel 44/2 onderling of met andere gegevensbanken waartoe de politiediensten toegang hebben door of krachtens de wet of internationale verdragen die België binden): "**Richtlijn koppeling**"
(iv) Article 44/4, § 6 van de WPA (Richtlijn betreffende de koppeling of de correlatie van de technische gegevensbanken): "**Richtlijn koppeling/correlatie TGB"**

6. Het Controleorgaan zal per richtlijn en voor het ontwerp van fiche CO2 een apart advies uitbrengen. Uiteraard moeten deze adviezen samen gelezen worden voor een goed begrip van de hele thematiek.

Het voorwerp van het advies betreft een gemeenschappelijke richtlijn – hierna aangeduid als 'de richtlijn informatieveiligheid' – waarin de aanvragers bij de toepassing van artikel 44/4 § 2 WPA de maatregelen vastleggen die nodig zijn om het beheer en de veiligheid, waaronder in het bijzonder de aspecten met betrekking tot de betrouwbaarheid, de vertrouwelijkheid, de beschikbaarheid, de traceerbaarheid en de integriteit van de persoonsgegevens en de informatie die in de Algemene Nationale Gegevensbank ('ANG'), de basisgegevensbanken, de bijzondere gegevensbanken en de technische gegevensbanken worden verwerkt, te verzekeren. De richtlijn is dwingend of bindend voor de geïntegreerde politie zoals dat het geval is voor de 4 voor advies voorgelegde ontwerpen van richtlijnen.

7. De opdracht tot het opstellen van deze richtlijn werd aan de politieministers opgelegd door de wet van 18 maart 2014[8]. Daarna werden de bepalingen met betrekking tot het informatiebeheer van de WPA gewijzigd en/of vervangen door de wet van 22 mei 2019 "*tot wijziging van diverse bepalingen wat het politionele informatiebeheer betreft*" (afgekort 'Wet politioneel informatiebeheer 2019')

(iii) Artikel 44/4 §§ 4 et 5 (Richtlijn betreffende de koppeling van de gegevensbanken bedoeld in artikel 44/2 onderling of met andere gegevensbanken waartoe de politiediensten toegang hebben door of krachtens de wet of internationale verdragen die België binden)
(iv) Article 44/4, § 6 van de WPA (Richtlijn betreffende de koppeling of de correlatie van de technische gegevensbanken)
Wij maken u tevens voor advies het ontwerp van fiche CO2 van de MFO3 betreffende de te nemen maatregelen over, gelet op het verband van deze fiche met de koppelingen en correlaties met de technische gegevensbanken. Zoals u weet dienen twee van deze richtlijnen gepubliceerd te worden in het Belgisch staatsblad, te weten (i) de Richtlijn met betrekking tot de toegang tot de ANG, de basisgegevensbanken, de bijzondere gegevensbanken en de technische door de leden van de politiediensten en (ii) deze met betrekking de koppeling van de gegevensbanken bedoeld in artikel 44/2 onderling of met andere gegevensbanken waartoe de politiediensten toegang hebben door of krachtens de wet of internationale verdragen die België binden".

[8] Art. 10 van de Wet van 18 maart 2014 "*betreffende het politionele informatiebeheer en tot wijziging van de wet van 5 augustus 1992 op het politieambt, de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en het Wetboek van strafvordering*".

teneinde de bepalingen met betrekking tot het informatiebeheer in overeenstemming te brengen met de *LED* en titel 2 WGB. De inhoud van de bepaling inzake de opdracht aan de politieministers om een richtlijn op te stellen, bleef nagenoeg ongewijzigd, maar werd uitgebreid met de aanvullende voorwaarde dat de richtlijn dwingend is voor de geïntegreerde politie[9].

III. BESPREKING VAN DE AANVRAAG

8. Binnen het kader van het politionele informatiebeheer maakt de geïntegreerde politie gebruik van nieuwe informatie- en communicatietechnologieën. Zoals in de richtlijn wordt aangegeven, moet daarbij de nodige aandacht worden besteed aan informatieveiligheid omdat dit een wezenlijk en onlosmakelijk aspect is van de bescherming van de persoonsgegevens. Het betreft een wettelijke basisplicht die in de artikelen 28, 6°, 50 en 51 WGB is verankerd. Artikel 44/4 § 2 WPA vereist in dat verband dat de politieministers de nodige maatregelen vastleggen om aan deze wettelijke vereisten te voldoen. Aldus moeten deze wettelijke verplichtingen in de richtlijn geconcretiseerd worden.

9. In de richtlijn worden de minimale beveiligingsmaatregelen vastgelegd, onderverdeeld in 17 aspecten (sub-rubrieken). Het gaat om een selectie van objectieven uit de *guidelines* van het Centrum voor Cybersecurity (*Baseline Information Security Guidelines*), met name:

1) het informatiebeleid en de beveiligingsplannen;
2) de organisatie van de informatieveiligheid;
3) de veiligheid inzake het personeelsbeheer;
4) sensibilisering, opleiding en communicatie;
5) het beheer van de activa;
6) de toegangscontrole;
7) cryptografie;
8) de fysieke veiligheid;
9) operationele veiligheid;
10) de beveiliging van de mededeling van de informatie;
11) aankoop, ontwikkeling en onderhoud van informatiesystemen;
12) betrekkingen met derden (leveranciers, autoriteiten);
13) het gebruik van een *Cloud*;
14) *incident management* aangaande informatieveiligheid;
15) informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer;
16) juridische monitoring;
17) evaluatie van de beveiligingsmaatregelen.

[9] En de toevoeging van "*onverminderd de eigen bevoegdheden van de gerechtelijke overheden*" (art. 7 wet van 22 mei 2019).

Hoewel deze aanbevelingen inderdaad als *best practices* zijn te beschouwen, moeten deze, zoals hiervoor opgemerkt, concreter worden uitgewerkt op het niveau van de politiediensten.

10. Bij wijze van algemene opmerking stelt zich ook hier de vraag naar de verhouding tussen deze richtlijn informatieveiligheid en de richtlijnen in de omzendbrief MFO-3. Wordt deze laatste vervangen door deze richtlijn voor alle aspecten van informatieveiligheid dan wel blijven de beide teksten naast elkaar bestaan? Daaromtrent duidelijkheid scheppen is in de eerste plaats voor de GPI van fundamenteel belang. Het sinds jaar en dag niet meer *up to date* houden van de MFO 3, wat toch de bijbel is van de politionele informatiehuishouding, aan het voortdurende wijzigende wettelijk kader is reeds ettelijke jaren een belangrijk pijnpunt. Dat wordt niet geremedieerd door de 4 ontwerpen van richtlijn. Integendeel, er is nu een bijkomende vraag, met name hoe deze 4 ontwerpen zich verhouden tot de bestaande dwingende regels van de MFO 3. Geen van de 4 richtlijnen brengt hieromtrent duidelijkheid. Het komt de steller van de ontwerpen toe hieromtrent klaarheid te scheppen.

Vervolgens stelt het COC zich de vraag of de richtlijn voldoende transparantie biedt in lijn met de verdragsrechtelijke grondrechten en verplichtingen zoals opgenomen in artikel 8 EVRM en de artikelen 7 en 8 van het EU Handvest van de Grondrechten. Op verschillende plaatsen in de richtlijn worden de relevante wettelijke bepalingen van de WGB, WPA en de objectieven van de aanbevelingen (quasi letterlijk) overgenomen of geparafraseerd zonder deze concreter uit te werken naargelang de context en het niveau (federale politie dan wel lokale politie) van de uitvoering. Zoals de richtlijn stelt, gaat het om "*minimale maatregelen waarmee de politiediensten rekening moeten houden bij het implementeren en evalueren van het informatieveiligheidsbeleid, de beveiligingsplannen en de procedures en de processen die daaruit voortvloeien*"[10]. Deze *Baseline Information Security Guidelines* zijn op zichzelf algemene doelstellingen die nader moeten ingevuld worden. Hoewel het COC begrijpt dat omwille van operationele en strategische redenen bepaalde aspecten in een interne richtlijnen worden uitgewerkt, dient de gepubliceerde richtlijn toch meer inzicht te brengen in de conformiteit van het beheer en de veiligheid van de informatie van de politiediensten. Immers, zoals in de richtlijn wordt gesteld, willen de politieministers met de maatregelen die in de richtlijn zijn opgenomen, onder meer, "*de veiligheid van haar personeel en de burgers (te) verzekeren en zo het vertrouwen van de maatschappij ten opzichte van hen te versterken*"[11]. Bijgevolg kan het COC zich in het advies onmogelijk over alle objectieven ten gronde uitspreken. De verdere uitwerking van de gestelde objectieven dient dan ook voor het COC ter beschikking te worden gehouden.

11. In de richtlijn worden de minimale beveiligingsmaatregelen vastgelegd. Het informatieveiligheidsbeleid wordt gevalideerd door het "*coördinatiecomité van de geïntegreerde politie*", zoals bedoeld in artikel 8*ter* van de WGP, na advies van het "*comité informatie en ICT*". De

[10] Rubriek " *II. INLEIDING*", p. 3.

[11] Rubriek " *II. INLEIDING*", p. 2.

beveiligingsplannen, die de concrete uitwerking van het veiligheidsbeleid bevatten, worden daarentegen op het niveau van de politiezone of de entiteit van de federale politie gevalideerd[12]. Het COC onderschrijft deze gedifferentieerde aanpak waarbij een uniform veiligheidsbeleid voor de geïntegreerde politie wordt vastgelegd en waarbij de uitwerking ervan context en plaatsgebonden worden ingevuld naargelang de organisatorische en technische middelen van de politiediensten.

12. Aangezien de functionaris voor de gegevensbescherming (DPO[13]) belast is met de opvolging van het informatieveiligheidsbeleid en de implementatie van het beveiligingsplan (of -plannen) stipt het COC aan dat de (operationele) verwerkingsverantwoordelijke er moet zorg voor dragen dat de DPO over de nodige kennis en expertise op het vlak van het persoonsgegevensbeschermingsrecht en informatieveiligheid beschikt en deze op peil wordt gehouden door het volgen van de (aanvullende) gespecialiseerde opleidingen. Dat is een verplichting die los staat van de sensibilisering, de opleiding en de communicatie van de personeelsleden van de politiediensten die in de richtlijn wordt vastgelegd. Een goede communicatie en verstandhouding tussen functioneel beheerder, korpschef of directeur, operationele directeuren en de DPO is op dat vlak primordiaal. Het Controleorgaan stelt in de praktijk vast dat het op dat vlak nog wel eens mank durft te lopen.

13. Het objectief "*3) De veiligheid inzake personeelsbeheer*" omvat het beleid en procedures inzake aanwerving, de tewerkstelling en de beëindiging of de verandering van dienstverband. Er moet opgemerkt worden dat deze aspecten in verband kunnen staan met verwerkingen die onder de toepassing van de AVG en titel 1 WGB vallen. Daardoor kan verwarring ontstaan omdat de richtlijn een uitwerking is van artikel 44/4 § 2 WPA en dus, in beginsel, louter betrekking heeft op operationele verwerkingen, met name verwerkingen die niet onder de AVG vallen, maar kaderen binnen de opdrachten van bestuurlijke en gerechtelijke politie (*LED* en titel II WGB). Dat geldt ook voor de objectieven "*Het beheer van de* activa" (sub-rubriek 5), de "*Aankoop, ontwikkeling en onderhoud van informatiesystemen*" (sub-rubriek 11) en "*Betrekkingen met derden (leveranciers, autoriteiten)*" (sub-rubriek 12) die niet noodzakelijk (volledig) in verband staan met operationele verwerkingen. Indien deze objectieven ook betrekking hebben op AVG-verwerkingen dient de steller van de richtlijn hierin duidelijkheid te brengen, minstens door de titel van de richtlijn in die zin uit te breiden en dit in de inleiding van de richtlijn te motiveren en te duiden.

14. Voor de regels inzake de toegang tot de persoonsgegevens en informatie in de politionele gegevensbanken verwijst de richtlijn naar een andere richtlijn zoals bedoeld in artikel 44/4 § 3 WPA (richtlijn toegangsregels). Hoewel het COC dit onderscheid kan begrijpen stelt zich in dat verband toch de vraag wat wordt bedoeld met de "*andere essentiële ICT-activa*"[14]. In zoverre daarmee ook

[12] Met name, respectievelijk, de korpschef en het directiecomité van de federale politie.

[13] *Data Protection Officer*.

[14] De richtlijn, p. 7 ("*6) de toegangscontrole*").

systemen of applicaties worden bedoeld die niet in verband staan met operationele verwerkingen wordt de steller van de richtlijn gevraagd daarin duidelijkheid te brengen.

15. De richtlijn besteedt ook kort en op algemene wijze aandacht aan cryptografie, het gebruik van clouddiensten en de plicht om ter zake adequate veiligheidsmaatregelen te nemen. Het COC brengt in dat verband het door de Europese Toezichthouder voor Gegevensbescherming (EDPS) uitgevoerd onderzoek onder de aandacht waarin enkele pijnpunten worden blootgelegd bij het opstellen van contracten voor de dienstverlening en producten van *Microsoft* aan EU-instellingen[15]. Zo werden onder meer tekortkomingen vastgesteld in de verwerkingsovereenkomst, met name het ontbreken van duidelijke instructies aan de verwerker en controle over de sub-verwerkers (verwerker van de verwerker) die door *Microsoft* onder de arm worden genomen, gemis aan zinvolle auditrechten voor de verwerkingsverantwoordelijke, het gebrek aan waarborgen en controle over de locatie, internationale transfers van de gegevens en het gevaar van onrechtmatige onthulling van de gegevens en het inbouwen van adequate technische oplossingen die een ongeautoriseerde gegevensflux naar *Microsoft* verhinderen. Zonder meer belangrijke aandachtspunten dus waarbij grote risico's op het vlak van de effectieve vertrouwelijkheid, de beschikbaarheid en integriteit van de politionele gegevens (persoonsgegevens en informatie) niet denkbeeldig zijn. Het Controleorgaan roept hieromtrent de GPI in het algemeen en de DRI[16] van de federale politie in het bijzonder op tot grote waakzaamheid.

16. Onder de rubriek 10, "*beveiliging van de mededeling van de informatie*", wordt gesteld dat afzonderlijke ministeriële richtlijnen hieromtrent werden uitgevaardigd. Het COC weet niet welke ministeriële richtlijnen worden bedoeld. Zij werden ook niet voorgelegd aan het Controleorgaan voor advies.

17. Tot slot begrijpt het COC niet de draagwijdte van de laatste rubriek "*IV. De methodologie*" in de richtlijn. Er wordt in algemene woorden verwezen naar "*de methodologie*" zonder concreet te stellen wat deze inhoudt, behalve dan dat deze moet gebaseerd zijn op de *Baseline Informatie Security Guidelines* van het Belgische Centrum voor Cybersecurity. Er moet worden opgemerkt dat deze *guidlines* geen bepaalde methodologie vooropstellen, laat staan, zoals in randnummers 9 opgemerkt, enigszins concretiseren. De steller van de richtlijn wordt bijgevolg gevraagd ter zake meer duidelijkheid te verschaffen.

18. Voor het overige heeft het COC geen specifieke opmerkingen.

OM DEZE REDENEN,

---

[15] EDPS, "*Outcome of own-initiative iventigations into EU institutions' use of Microsoft products and services* 2 juli 2020, https://edps.europa.eu/data-protection/our-work/publications/papers/outcome-own-initiative-investigation-eu-institutions_en.

[16] Directie van de politionele informatie en de ICT-middelen.

Het Controleorgaan op de Politionele Informatie,

verzoekt gevolg te geven aan het gestelde onder randnummers 10 tot en met 17 ;

verzoekt voor het overige rekening te houden met de andere hogervermelde opmerkingen.

Aldus goedgekeurd door het Controleorgaan op de Politionele Informatie op 22 september 2020.

Voor het Controleorgaan,
De voorzitter,
(get.) Philippe ARNOULD